ENDEAVOUR ACADEMIES
POLICIES

INSPIRING FUTURES

ONLINE SAFETY POLICY

Macmillan Academy
Post 16 Macmillan Academy
PRIMARY SCHOOL ARCHIBALD

POLICY DETAILS

Policy title:	Online Safety Policy
Staff name and job title:	Mr A King – Deputy Headteacher
Organisation:	Endeavour Academies
Policy version number:	1.2
Approval date:	May 2023
Date of Next Review:	May 2024
Distribution:	Website

POLICY REVISION AND APPROVAL HISTORY

Version	Date of review	Date of next review	Comments	Approved by
1.1	October 2022	October 2023	Changes made to expectations of all staff within the trust (Cyber Security training). Changes to protocols for new social media accounts. Change from Data Protection Act to GDPR	Headteacher
1.2	May 2023	May 2024	Revised policy to become Trust Policy	CEO

CONTENTS

1. INTRODUCTION

1.1 The purpose of this policy is to:

- Set out the key principles expected by Endeavour Academies of all members of Trust community with respect to the use of ICT-based technologies
- Safeguard and protect the children and staff of the Trust
- Highlight issues affecting the use of ICT-based communication systems
- Assist Trust staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal, or recreational use
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other Trust policies
- Ensure that all members of the Trust community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with students
- State the actions that may be taken to monitor the effectiveness of this policy suite
- Warn users about the consequences of inappropriate use of ICT-based technology and systems
- Establish a framework within which users of the Trust and academies ICT-based facilities can apply self-regulation to their use of ICT systems.

2. SCOPE OF THE POLICY

This policy applies to all members of the Trust community (including staff, students/pupils, trustees/governors, parents/carers, visitors, community users) who have access to and are users of Trust/academy digital technology systems, both in and out of the Trust.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students/pupils 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 online bullying or other online safety incidents covered by this policy, which may take place outside of the Trust, but is linked to membership of the Trust. 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.

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 online safety behaviour that take place.

3. ROLES AND RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust. In addition to the roles and responsibilities below, all staff within the trust are required to have completed cyber security training provided by the National Cyber Security Centre.

3.1 Local Governing Body/Board of Trustees

Trustees are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about online safety incidents and monitoring reports. A member of the Academy Governors has taken on the role of Child Protection/Safeguarding which also covers *Online Safety*. The role will include:

- regular meetings with the Academy DSL
- attendance at relevant safeguarding meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering
- reporting to relevant Academy Council/Board/Committee/meeting

3.2 Academy Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.
- The Headteacher and (at least) another member of the Senior Leadership should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/MAT/other relevant body disciplinary procedures).
- The Headteacher/Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online 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 Designated Safeguarding Lead.

3.3 Academy Designated Safeguarding Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Trust/relevant body
- liaises with Trust/academy technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Liaise with the governing body to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings
- reports regularly to Senior Leadership Team

3.4 Network Manager/ICT Technical staff

The Network Manager/ICT Technical Staff is responsible for ensuring:

- that the technical infrastructure is secure and is not open to misuse or malicious attack
- that the Trust meets required online safety technical requirements and any Online Safety Policy/Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see "Technical Security Policy" for good practice)
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/internet/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Network Manager/Headteacher/Senior Leader/DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated

3.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Trust Online Safety Policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Network Manager/Headteacher/Senior Leader/DSL for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/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 school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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

3.6 Designated Safeguarding Lead/Designated Person/Officer

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

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

3.7 Students/Pupils:

- are responsible for using the academy digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- 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 policies on the use of mobile devices and digital cameras.
- They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

3.8 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. The Trust will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support the Trust in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to online safety sections of the website

3.9 Community Users

Community Users who access Trust systems/website as part of the wider Trust/academy provision will be expected to sign a Community User AUA before being provided with access to Trust/academy systems.

4. POLICY STATEMENTS

4.1 Education – Students/Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students/pupils* to take a responsible approach. The education of *students/pupils* in online safety/digital literacy is therefore an essential part of the Trust's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students/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
- Students/pupils should be helped to understand the need for the student/pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside their academy
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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

4.2 Education – Parents/Carers

Many parents and carers have only a limited understanding of online 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Trust 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. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

4.3 Education – The Wider Community

The Trust will provide opportunities for local community groups/members of the community to gain from the Trust's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their Online Safety provision

4.4 Education and Training – Staff/Trustees/Academy Council Governors

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

- A planned programme of formal safeguarding training will be made available to staff. This will be regularly updated and reinforced
- All new staff should receive safeguarding training as part of their induction programme, ensuring that they fully understand the Trust Online Safety Policy and Acceptable Use Agreements
- It is expected that some staff will identify online safety as a training need within the performance management process
- The DSL (or other nominated person) will receive regular updates through attendance at external training events (e.g. from LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The DSL (or other nominated person) will provide advice/guidance/training to individuals as required

4.5 Training – Governors/Trustees

Academy Intervention staff should take part in safeguarding training/awareness sessions, with particular importance for those who are members of any subcommittee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Trust/Local Authority/National Governors Association/or other relevant organisation
- Participation in Trust/academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons)

4.6 Technical – infrastructure/equipment, filtering and monitoring

The Trust will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Trust technical systems and devices.
- All users will be provided with a username and secure password by the Academies ICT Manager or ICT Technician *who will keep an up to date record of users and their usernames.* Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the Trust/academy ICT systems, used by the Academies ICT Manager (or other person) must also be available to the *Network Manager* and kept in a secure place
- The Academies ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet

- The Trust has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc.)
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software
- The provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems must be agreed by the Academies ICT Manager, Trust ICT Manager or Network Manager
- Users are forbidden from downloading executable files and installing programmes on Trust devices without the express permission of the Trust ICT Manager or Academies ICT Manager
- The use of removable media (e.g. memory sticks/CDs/DVDs) by users on Trust/academy devices is discouraged. Personal data cannot be sent over the internet or taken off the Trust/academy site unless safely encrypted or otherwise secured
- For further information on information security please refer to the following Trust policies: *Data Protection Policy, GDPR Policy.*

4.7 Mobile Technologies (including BYOD)

All users should understand that the primary purpose of the use mobile/personal devices in an academy context is educational. The use of mobile technologies should be consistent with and interrelated to other relevant Trust polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage.

4.7.1 Staff use of personal devices

Staff using personally owned devices (mobile phones/laptops) for work use:

- Are subject to audit checks if mobile expenses claims are submitted
- Must ensure the mobile device is pin code/password protected at all times with a screen lock
- Must not allow another person to access their mobile device for any reason to ensure there is no risk to any sensitive data stored on the device
- Must ensure remote deletion of data is setup in case the device is lost or stolen (e.g. Apple's 'Find iPhone')
- Where staff members are required to use a mobile phone for Trust duties, for instance in case of emergency during offsite activities, or for contacting students or parents, then a Trust mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a Trust owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes

4.8 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The Trust will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press
- It is at the academy Headteacher's discretion to allow parents/carers to take videos and digital images of their children at school/academy. If permission is granted by the Headteacher, 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 students/pupils in the digital/video images.
- Staff are allowed to take digital/video images to support educational aims, but must follow Trust/academy policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers

4.9 Data Protection

Personal data must be recorded, processed, transferred and made available according to current data protection legislation.

The Trust must ensure that:

- It has a GDPR/Data Protection Policy
- It has paid the appropriate fee to the Information Commissioner's Office (ICO)
- It has appointed a Data Protection Officer (DPO)
- Data Protection Impact Assessments (DPIA) are carried out where appropriate
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers
- Policies must cover the right of the data subject to access their information (subject access requests)
- There are clear and understood data retention policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from data protection breaches which recognises the requirement to report relevant data breaches to the ICO within 72 hours of identification, where feasible
- Consideration has been given to the protection of personal data when accessed using any remote access solutions
- It must have a Freedom of Information Policy which sets out how it will deal with FOI requests
- All staff receive data handling awareness/data protection training at least annually (or on induction for new staff) and are made aware of their responsibilities

The academy must ensure that:

- It has identified a Data Protection lead, who will act as the first point of contact for day-to-day issues and questions that may arise
- It retains a log of subject access requests and information disclosures, with reasons and description of information disclosed as appropriate
- It will hold the minimum personal data necessary to enable it to perform its function, it will not hold it for longer than necessary and will use it only for the for the purposes for which it was collected
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay
- Data protection/information handling training is scheduled at least annually and is part of induction for new staff
- It has an information asset register for all paper-based information systems
- It adheres to all policies relating to information security and data protection and it publishes the privacy notice and relevant policies on its website

Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk
- Understand the process for dealing with subject access requests
- Understand what constitutes a data protection breach and know how to report breaches that occur
- Take adequate precautions when sharing paper-based information to keep it secure, e.g. asking others to check postal addresses/contents when sending confidential documents to parents etc.
- Use electronically-stored 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
- In very exceptional circumstances when personal data is stored on any portable computer system, memory stick or any other removable media:
  - The data must be encrypted and password protected
  - The device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
  - The device must offer approved virus and malware checking software o The data must be securely deleted from the device, in line with Trust policy once it has been transferred or its use is complete

4.10 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

4.10.1 When using communication technologies, the Trust considers the following as good practice:

- The official Trust email service (Microsoft 365) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students/pupils should therefore use only the Trust email service to communicate with others
- Users must immediately report, to the nominated person – in accordance with the relevant policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs etc.) must be professional in tone and content. These communications may only take place on official (monitored) Trust systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school/academy email addresses for educational use
- Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with

inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the Trust/academy website and only official email addresses should be used to identify members of staff

4.11 Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Academies and MATs could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the Trust or academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

4.11.1 The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Trust 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

4.11.2 Trust staff should ensure that:
- No reference should be made in social media to students/pupils, parents/carers or Trust/academy 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

4.11.3 When official Trust 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.
- Usernames and passwords for all social media accounts should be shared as a backup with the designated member of the senior leadership team for IT management.

4.11.4 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 Trust or impacts on the Trust, it must be made clear that the member of staff is not communicating on behalf of the 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 school 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 Trust permits reasonable and appropriate access to private social media sites

4.11.5 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 the Trust
- The Trust should effectively respond to social media comments made by others according to a defined policy or process

4.11.6 The Trust's use of social media for professional purposes will be checked regularly by the Trust Compliance & Communications Officer to ensure compliance with the Trust policies.

4.12 Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Trust and all other technical systems. Other activities e.g. cyberbullying would be 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 Trust/academy context, either because of the age of the users or the nature of those activities.

The Trust believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in/or outside the academy when using Trust/academy equipment or systems. The Trust policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and 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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

4.13 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

4.14 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 *appendix "Responding to incidents of misuse – flow chart"* for responding to online safety incidents and report immediately to the police.

4.15 Other Incidents

It is hoped that all members of the Trust community will be responsible users of digital technologies, who understand and follow Trust policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

4.15.1 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
- Police involvement and/or action.

4.15.2 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
- other criminal conduct, activity or materials**.**

4.15.3 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 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.

4.16 Trust/Academy Actions & Sanctions

It is more likely that the Trust/academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Trust 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.

5. FURTHER GUIDANCE

Schools in England (and Wales) are required *"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, 2015).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead*

to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

In response UKSIC produced guidance on – information on "Appropriate Filtering"
NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-esecuritycyber-security-in-schools/

6. LEGISLATION

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

6.1 Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

6.2 GDPR

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. For all organisations processing personal data, the following seven protection principles apply:

- **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation** — You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization** — You should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy** — You must keep personal data accurate and up to date.
- **Storage limitation** — You may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

6.3 Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

6.4 Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

6.5 Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

6.6 Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication.

Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.

- The school reserves the right to monitor its systems and communications in line with its rights under this act.

6.7 Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

6.8 Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. Youtube).

6.9 Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

6.10 Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

6.11 Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

6.12 Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

6.13 Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

6.14 Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or

travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

6.15 Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

6.16 Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

6.17 Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

6.18 The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

6.19 The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data – http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screeningsearching-and-confiscation)

6.20 The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems.

6.21 The School Information Regulations 2012

Requires schools to publish certain information on its website: https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

6.22 Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including Child Sexual Exploitation).

7. APPENDICES

Student / Pupil Acceptable Use Agreement
Student / Pupil Acceptable Use Agreement Form
Student / Pupil Acceptable Use Policy Agreement - KS1
Staff Acceptable Use Policy Agreement
Trustee / Governor Acceptable Use Policy Agreement
Acceptable Use Agreement for Community Users
Online Safety Policy - Responding to incidents of misuse flow chart

Student/Pupil Acceptable Use Agreement

Trust/Academy Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. 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 at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the Trust/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 on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line

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

- I understand that the Trust/academy 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 Trust/academy systems or devices for on-line gaming, on-line gambling, 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 school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Trust/academy:

- I will not only use my own personal devices (mobile phones, USB devices, etc.) in school
- 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 school device, nor will I try to alter computer settings

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 school:

- I understand that the Trust/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 school and where they involve my membership of the school 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 school 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 school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the *student/pupil* 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 school systems.

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

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

Name of Student/Pupil:	
Group/Class:	
Signed	
Date:	

Student/Pupil Acceptable Use Policy Agreement - KS1

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/tablets
- 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/tablet

The academy will discuss this Acceptable Use Agreement with KS1 pupils and provide online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Staff Acceptable Use Policy Agreement

Trust Policy

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 at all times.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that Trust/academy 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 technology in their everyday work

The Trust/academy will try to ensure that staff will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the Trust/academy will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g.
  laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology 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/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 steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

I will be professional in my communications and actions when using *Trust/academy* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the Trust/academy website) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use social networking sites in school in accordance with the Trust/academy's policies
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Trust/academy:

- When I use my mobile devices (laptops, tablets, mobile phones, USB devices, etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *Trust/academy* equipment. I will also follow any additional rules set by the *Trust/academy* about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses
- I will not use personal email addresses on the Trust/academy 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 my data is regularly backed up, in accordance with relevant Trust/academy policies
- 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 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 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 this is allowed in school / academy policies
- I will not disable or cause any damage to Trust/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 Trust/Academy/GDPR 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
- I understand that data protection policy requires that any staff or student/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 Trust/academy policy to disclose such information to an appropriate authority
- 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 Trust sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of the Trust/academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust/academy digital technology equipment in school, but also applies to my use of

Trust/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Trust/academy

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

I have read and understand the above and agree to use the Trust digital technology systems (both in and out of academy's) and my own devices (when carrying out communications related to the Trust) within these guidelines.

Staff name	
Signed	
Date:	

Trustee/Governor Acceptable Use Policy Agreement

Trust Policy

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 people to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that trustees/governors will be responsible users and stay safe while using the internet and other communications technologies for purposes related to their governance role
- that Trust systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that trustees/governors are protected from potential risk in their use of technology in their everyday work

The Trust will try to ensure that trustees/governors will have good access to digital technology to enhance their role, and will in return, expect trustees/governors to agree to be responsible users.

Agreement to the Acceptable Use Policy

I understand that I must use Trust systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my professional and personal safety:

- I understand that the Trust will monitor my use of the digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the Trust digital technology 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 · 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 steal it

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person

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

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

The Trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Trust/academy:

- When I use my mobile devices (laptops, tablets, mobile phones, USB devices, etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using Trust equipment. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses
- I will not use personal email addresses on the Trust 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 my data is regularly backed up, in accordance with relevant Trust policies
- 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 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 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 this is allowed in Trust policies
- I will not disable or cause any damage to Trust/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 GDPR 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
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority
- 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 Trust-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of the Trust/academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust digital technology
  equipment in school, but also applies to my use of Trust systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my position on the academy council
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees, and in the event of illegal activities, the involvement of the police

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

Name:	
Signature:	
Date:	

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of Trust/academy digital technologies will be responsible users and stay safe while using these systems and devices
- that Trust / 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 Trust 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 the Trust/academy:

- I understand that my use of Trust/academy systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into the Trust/academy's 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, without permission. 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 school on any personal website, social networking site or through any other means, unless I have permission from the school
- 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 a Trust 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 Trust/academy 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 Trust/academy has the right to remove my access to Trust systems/devices.

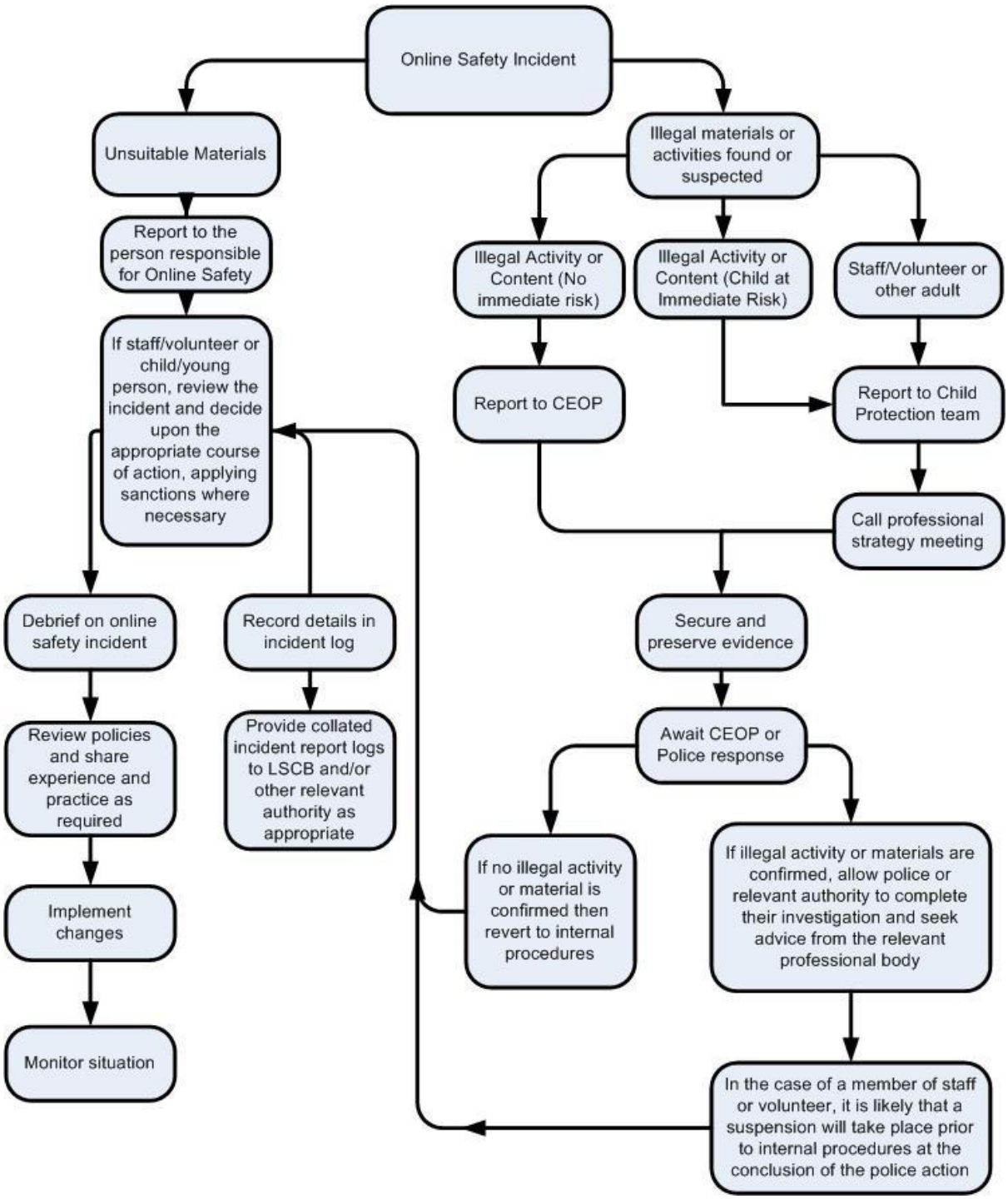
I have read and understand the above and agree to use the Trust digital technology systems (both in and out of school) and my own devices (when carrying out communications related to the Trust) within these guidelines.

Name: _____

Signed: _____

Date: _____

Online Safety Policy - Responding to incidents of misuse flow chart



ENDEAVOUR ACADEMIES

Stockton Road
Middlesbrough
TS5 4AG

01642 800800

enquiries@endeavour-academies.org.uk
www.endeavour-academies.org.uk

Macmillan Academy
Post 16 Macmillan Academy
Primary School ARCHIBALD