NINESTILES
ACADEMY TRUST

Ninestiles Academy Trust Mission Statement

Ninestiles Academy Trust will be nationally and internationally acknowledged as a high achieving, innovative and exciting group of schools which recognise and respect the richness and diversity of their communities. The trust will be structured and resourced to meet the needs of 21st century students and pupils. Within a caring environment, we will develop and reinforce the values, skills and attributes which promote good citizenship and lifelong learning. Parents, directors, academy councillors, and the wider community will work in partnership with our committed, appropriately skilled workforce and our students and pupils, to ensure that high quality learning takes place.
Outcomes will be outstanding.

Policy title	**E-Safety Policy**
Rationale	**1. Introduction** The Ninestiles Academy Trust: • Contributes to high quality teaching and learning • Enables effective tracking, target setting and the management of intervention strategies • Enables focused assessment • Supports effective internal and external communication. However, there are inherent dangers of using this powerful tool in a school environment. It is therefore essential that schools create a safe ICT learning environment that includes three main elements: • An effective range of technological tools • Policies and procedure to describe and maintain the acceptable use of the schools ICT services and facilities with clear roles and responsibilities • a comprehensive e-Safety education programme for students, staff and parents. The e-Safety policy has been written in accordance with our vision for the Ninestiles Academy Trust and is supported by the following school policies: Anti-Bullying Policy, Behaviour Policy, Child Protection, Complaints Policy, and marking and assessment policy.

Policy statement	**2. Key Principles** • All students should be able to learn in a safe environment and should not be exposed to inappropriate materials or cyber-bullying • All staff are responsible for promoting and supporting safe behaviours in their classrooms and following the Ninestiles Academy Trust's e-Safety policy • There is a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials for investigation. **3. Aims** • To ensure students can learn in a safe and secure environment, in and out of school • To minimise the risk of student exposure to inappropriate material or cyber-bullying • To develop secure practice for students when communicating electronically • To develop student self-responsibility when communicating electronically • To ensure consistent good practice for staff when communicating electronically • To ensure all staff are aware of issues relating to e-Safety • To provide information, advice and guidance for parents/carers on the use of new technologies. **4. Roles and Responsibilities** ***Board of Directors:*** • Ensure the e-Safety Policy is implemented, monitored and reviewed ***Trust Leadership Teams:*** • Ensure, along with the Academy Councils that the e-Safety Policy is implemented, monitored and reviewed. • Ensure that all staff are aware of their responsibilities under the policy and are given appropriate training and support so that they can fulfil their responsibilities • Ensure that issues of e-Safety, including cyber-bullying, are addressed within the curriculum Schools' e-Safety Officer ***Schools' ICT teams*** • Ensure the School remains 'up to date' with e-Safety issues and guidance through organisations such The Child Exploitation and Online Protection (CEOP) • Ensure the Principal is updated as necessary, including being aware of local and national guidance on e-Safety and they are updated at least annually on policy developments • Ensure the School Network is safe and secure for all groups – consistent application of protocols and management and development of software • Advise Academy Council/Leadership Team on e-Safety issues/technology Teachers/Tutors/mentors/teaching assistants * Responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures **5. The School Network** The security of the School Network is maintained by: • Ensuring its health through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc. • Ensuring it is 'healthy' though robust monitoring on the network (these may be replaced or updated as appropriate to take account of technical & commercial developments) • Ensuring the Network Manager is up-to-date with providers services for security • Ensuring that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately (responsibility of the Network Manager) • Not allowing students access to Internet logs • Using individual log-ins for students and all other users • Never sending personal data over the Internet unless it is encrypted or otherwise secured; or sent via secure systems such as the DfE s2s site • Ensuring students only publish within appropriately secure learning environments such as their own closed secure log-in **6. The Internet** Ninestiles Academy Trust schools recognise that access to the Internet is an invaluable

learning tool and vital for effective communication. Safety and security risks are minimised through:
• The use of the BGfL and internal filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature
• Effective planning - Internet use is matched to students' ability,
• Informing users that Internet use is monitored in the Acceptable Usage Agreement, and as part of our student induction process in ICT lessons
• Informing staff and students that that they must report any failure of the filtering systems directly to the Network Manager or the classroom teacher
• Blocking all Chat rooms and social networking sites except those that are part of an educational network
• Only using approved 'Blogging' or discussion sites,
• Requiring all staff are made aware of the Ninestiles Academy Trust Acceptable Use policy and that on signing their terms and conditions of employment they agree to comply with its contents.
• Ensuring all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through induction and teaching programme (refer to the Internet and email policy)
• Maintaining a record of any cyber-bullying or inappropriate behaviour (the e-Safety Log and the Behaviour Log) and act to deal with the perpetrators of this behaviour
• Making information on reporting offensive materials, abuse / bullying etc available for students, staff and parents
• Immediately referring any material suspected of being illegal to the Police
• Establishing that E Mail and Internet use is not private and the schools reserve the right to monitor all E Mails and Internet usage involving the school's IT facilities and/or services
• Allocating an E Mail account through the school domain – enabling them to access their E Mail from school and at home through web connect system
• Ensuring staff do not communicate with students via their personal Hotmail, MSN accounts or through their personal social networking site account (e.g. Facebook, Twitter etc.)
• Ensuring staff only communicate with students via their designated School E Mail account
• Ensuring staff do not attempt to use their personal social networking site(s) in school
• Ensuring staff do not communicate with, or have details of, students on their personal social net-working account or any other electronic device e.g. Facebook
• Ensuring that staff should not have student contact details on their personal mobile phones; except for the specific duration of a school trip/visit
• Ensuring that student details are always taken from CMIS, and any new contact details obtained being passed to the school office for updating as may be appropriate
• Making students aware of the risks and issues associated with communicating through E Mail and to have strategies to deal with inappropriate E Mails, as part of the school's e-Safety and anti-bullying education programme.

7. Digital and Video Images
To prevent the inappropriate use of images of students within the NINESTILES ACADEMY TRUST the following is observed:
• Notification is given to parents that school, may publish photographs, video footage etc of students. But will ensure that images of their child may be used to only to represent the schools or the Ninestiles Academy Trust
• Photographs published on the Internet do not have full names attached
• Digital images /video of students are stored securely .
• Students' names are not used when saving images in the file names or in the <ALT> tags when publishing to the school Website
• The Schools avoid including the full names of students in the credits of any published school produced video materials / DVDs; or anywhere that they can be easily identified from photos or videos
• The Principals take overall editorial responsibility for the website but delegate the operational day to day management to a named individual to ensure content is accurate and quality of presentation is maintained
• Uploading of information is delegated to individuals responsible for specified areas.
• The School Web Site complies with the Ofsted guidelines.
• Where other's work is published or linked to, the school credits the sources used and state clearly the author's identity or status
• The point of contact on the Website is the main school address and telephone number, or occasionally individual School domain contact details. Home information or individual private E Mail identities will not be published

	• Staff are made aware of the Acceptable Use in induction and on signing the terms of conditions on employment are agreeing to comply with the policy • Students are taught to be aware of the possible wide range of audiences and how images can be abused in their e-Safety education programme. **8. Cyber Bullying** The use of the Internet, text messages, E Mail, video or audio to bully another student or member of staff will not be tolerated. Bullying can be done verbally, in text or images e.g. graffiti, text messaging, E Mail or postings on websites. 'Cyber bullying' is a form of bullying via communication technology like text messages, E Mails or websites. It takes many forms - sending threatening or abusive text messages or E Mails, personally or anonymously, making insulting comments about someone on a website, social networking site (e.g. Facebook) or online diary (blog/Twitter), making, or sharing, derogatory or embarrassing videos of someone via devices or E Mail. It should be noted that the use of ICT to bully could be against the law. Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means), may be libellous and contravene the Harassment Act 1997 or the Telecommunications Act 1984. The nature and consequences of cyber-bullying are addressed in ICT/Aspire lessons at KS3 and 4. A range of strategies are recommended to support someone who is the victim of cyber-bullying. **9. Monitoring Arrangements** The trust will aim to ensure that all appropriate monitoring arrangements in relation to all Internet, E Mail and related services and facilities that it provides are in place and the schools will apply these monitoring arrangements to all users. These arrangements may include checking the contents of, and in some instances recording, E Mail messages for the purpose of: • establishing the existence of facts relevant to schools within the Ninestiles Academy Trust • ascertaining or demonstrating standards which ought to be achieved by those using the facilities • preventing or detecting crime • investigating or detecting unauthorised use of E Mail facilities • ensuring effective operation of email facilities • determining if communications are relevant to the School, for example where an employee or student is off sick or on holiday. The schools may, at their discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this Policy. These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the school's e-Safety Policy and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Disclaimer The school may arrange for an appropriate disclaimer to be appended to all E Mail messages that are sent to external addresses from the school, in order to provide necessary legal protection. **10. e-Safety Education** 10.1 Students An e-Safety programme is provided for all students on • How to stay safe • Social media • Cyber bullying At all Key Stages e-Safety forms a component of the assemblies. 10.2 Staff As part of their induction, all new staff are required to read the e-Safety policy. All staff are required to read the e-Safety Policy and the Acceptable Usage Policy. E-Safety up-dates are circulated by the e-Safety officers when received 10.3 Parents/Carers E-Safety Information is provided for parents. Advice and guidance can also be accessed via the Schools Web Sites. For example, a link has been established to allow parents to

	download the CEOP 'Parents and Carers Guide to the Internet'. Reminders will appear in the School Newsletter. **11. e-Safety Complaints** 11.1 Role of School Complaints should be dealt with in accordance with the Ninestiles Academy Trust Complaints Policy. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the Ninestiles Academy Trust child protection policy The schools take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a schools computer or mobile device. The schools cannot accept liability for material accessed, or any consequences of Internet access or ICT usage. 11.2 Investigation of Complaints The school will investigate complaints received from both internal and external sources, about any unacceptable use of ICT that involves the school IT facilities. External complaints will be addressed with reference to our Complaints Policy. The investigation of facts of a technical nature, e.g. to determine the source of an offending E Mail message, will be undertaken by the NINESTILES ACADEMY TRUST Network Manager in conjunction with other departments as appropriate. Where there is evidence of a criminal offence, consideration will be given to whether the issue will be reported to the police for them to take appropriate action. The schools will co-operate with the police and other appropriate external agencies as required in the investigation of alleged offences. In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then appropriate action will be taken (outlined in Appendix 11 of School e-Safety Policy, Protocol and Procedure document). 11.3 Action in the Event of a Breach of the Standards of Acceptable Use In circumstances where there is assessed to be a breach of the standards of acceptable use, the schools will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements, and will typically involve liaison between the appropriate member(s) of the Leadership Team and the Network Manager. Subsequent action will be as described below: • Indications of non-compliance with the provisions of the e-Safety Policy will be investigated, as appropriate, in accordance with the provisions of the school's Disciplinary Procedures, as applicable to staff and students • Subject to the findings of any such investigation, non-compliance with the provisions of the e-Safety Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct for staff members or exclusion for a student. Furthermore, publication, accessing or storing of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action • Complaints of cyber-bullying will be included be recorded and dealt with in accordance with our Anti-Bullying Policy • Complaints related to child protection are dealt with in accordance with the schools child protection procedures • In the case of child pornography being found, the person or persons suspected should be immediately suspended and the Police will called on 0808 100 00 40 • Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html.
Monitoring and review	Board of Directors

Links	Anti-Bullying Policy Behaviour Policy Child Protection Complaints Policy Assessment Policy
Staff responsible	CEO, Principals, SLG and staff within schools
Committee responsible	Board of Directors
Date approved	February 2016
Review date*	February 2018

**Please note that should any further national guidance be issued by external agencies that are relevant to this policy, it will be updated accordingly prior to the review date shown above and referred to the next academy council meeting*