esafety Policy

Review Period:	Annually
Date Policy Last Reviewed:	January 2018
Date of Governor Approval:	April 2018
Date for Review:	January 2019

1. Aim

The purpose of this e-safety policy is to outline the measures our Academy takes to ensure that students and staff can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

Within the Academy all members of staff and students are responsible for e-safety. Responsibilities for each group include:

Governors and Academy Senior Leadership

The governing board has overall responsibility for monitoring this policy and holding the head of school to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding officer.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The head of school and the senior leadership team are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Students

At The Academy of St Nicholas, students are also responsible for their own e-safety.

All students will:

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety lessons
- Compliance with the Student's Acceptable Use Policy (AUP) to which students must agree prior to use of academy ICT equipment either within the academy or remotely.
- Reporting any e-safety issue to the teacher, head of year or parent.
- Take responsibility for their own actions using the internet and communications technologies.
- Supporting the Academy in its eSafety activities by reinforcing acceptable use and e-behaviour messages

Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Having a clear understanding of e-safety issues and the required actions including
- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of Academy network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital
- cameras
- eBullying / Cyberbullying procedures
- Their role in providing e-Safety education for students
- Reporting any e-safety issues to the ICT team or Safeguarding team as soon as the issue is detected
- Compliance with the Staff Acceptable Use Policy (AUP) to which staff must agree prior to use of academy ICT equipment either in the academy or remotely.
- Educating students on e-safety and re-enforcing this in the day to day use of ICT in the classroom
- Fostering a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate material

ICT Technical Department

The ICT team is directly responsible for:

- Keeping up to date with e-Safety issues and guidance through liaison with the relevant organisations
- Updating the head of school, governors and senior management on e-Safety; providing information and instruction on an annual basis on policy developments, issues and strategies
- Referring any material believed to be suspect to the appropriate authorities e.g. Careline, Police, Safeguarding team
- Ensuring that the best filtering and monitoring systems solutions are in place to ensure e-safety whilst still enabling students to use the internet effectively in their learning.
- Ensuring that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e- safety breach
- Checking and auditing all systems to ensure that no inappropriate data is stored or is accessible
- Working with the safeguarding team to create, review and advise on e-safety and acceptable user policies

Parents

Parents are expected to:

- Notify a member of staff or the head of school of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head of school and/or the safeguarding team.

Concerns or queries about this policy can be raised with any member of staff or the head of school.

6. The Academy of St Nicholas E-Safety Policies

It is the duty of the Academy to ensure that every student, staff members and visitor in their care is safe using our technology. The Academy endeavours to ensure the e-safety of all academy members by using education, technology, accountability, responsibility and legislation to achieve this.

The Academy will therefore ensure that the following technologies are safe for students and staff to use by deploying the following approaches:

Internet

- Ensuring that the best filtering and monitoring systems solutions are in place to ensure e-safety whilst still enabling staff and students to use the internet effectively for teaching and learning
- Maintaining broadband connectivity through an accredited provider
- Working in partnership with the provider to ensure any concerns about the system are communicated effectively so that systems remain robust and protect students
- Use an industry recognised hardware firewall to protect staff and students from external threats
- Ensuring network security through anti-virus software and ensure network policies are in place so staff and students cannot download, save or run potentially harmful executable or media files
- Utilising Impero classroom monitoring software to observe real time desktop and laptop usage as well making use of its keywords function to alert the ICT team, safeguarding officers, teachers and heads of years of any live misuse so they can action any violations immediately
- Ensuring that the internet filtering system is performing its duty of automatically blocking any new emerging website it deems inappropriate by checking any reported sites are categorization against the existing banned categories list (e.g. pornography, radicalization) and blocking it if not correctly filed
- Using individual user accounts for students and all other users so individuals can be held accountable for their own internet usage
- Ensuring users, especially staff, do not send personal data over the Internet unless it is encrypted or otherwise secured
- Google Safe Search is enforced for all users to filter out inappropriate search content
- Incognito mode and In Private browsing are disabled for all users to ensure everyone's internet search history is recorded

Academy Website

With specific reference to publishing information on the St Nicholas' website:

- Only the ICT team will be granted rights to upload information and therefore have overall technical responsibility for the site
- Only excerpts will be published from student's work and all work will be checked to ensure no reference is made to named individuals, no infringements of copyright or other relevant legislation has occurred and, where applicable, appropriate credits has been given to information sources; editorial responsibility therefore lies with the member of staff submitting the work for publication.
- All links will be checked for suitability at the time of linkage and periodically after this to ensure continued suitability

Email

- Email addresses are configured and set by the ICT team and are checked for unsuitable content and viruses
- The Academy's internal Office 365 mail system is not considered private and the Academy reserves the right to monitor and access all users internal e-mail usage should legitimate concern be raised

- Communication between students, other students and staff must be for educational purposes only
- Attachments must only be approved file extensions such as .docx, .pdf, .ppt etc.
- Should a users internal email account need to be accessed due to concern the Academy will ensure the preservation of the users human rights and that all private data is secured.
- The use of personal e-mail accounts, such as Hotmail, should be avoided by all staff. Staff should use the Academy's systems wherever possible for professional purposes only.

Social Networking and Other Banned Content

- Social Network Sites are deemed inappropriate for use within the Academy and are blocked at source
- Sites requested for educational purposes will be checked and allowed through the filter if deemed appropriate by the ICT Team
- Downloads, media, gaming and shopping sites are all blocked within the Academy
- Streaming media from sites, such as YouTube, are permitted only for sixth form students and is enforced with Google Safe Search to filter out inappropriate content
- Sexual education content is permitted within reason and can be blocked or allowed by the ICT Team

Webcams and Video Conferencing

- Only staff are authorized to use such platforms within the Academy and are blocked at source for students
- Only approved video conferencing system services will be used.
- Only approved or checked webcam sites will be used.

Mobile and Smart Phones

The Academy will allow all mobile and smart phones to be used in line with its communications and behaviour for learning policies. Pupils may bring mobile devices into school for contact with parents/carers/guardians, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Must not be used on the corridors or in any of the school's outdoor areas.

Mobile phones should not be visible anywhere on school property. If seen they will be confiscated and held securely by the head of year. Heads of year will then contact home. Parents/carers can collect the mobile from school at the end of the day from the main office.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Safeguarding team or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Staff using work devices outside school

- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.
- Any USB devices used must not contain data relating to the school under as per the new GDPR guidelines.
- If staff have any concerns over the security of their device, they must seek advice from the ICT team.
- The ICT team must ensure all staff devices are BitLocker encrypted to ensure the data on the device's hard drive is secure should the staff device be lost or stolen
- Work devices must only be used for work activities

7. General ICT Code of Conduct

The Academy will take all reasonable precautions to ensure e-Safety. However when inappropriate use or infringement of policy is detected, the Academy will review the event and, if appropriate, implement sanctions in line with the following:

Students

Category A Infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups

Possible Sanctions: sanctioned in line with Academy Behaviour Policy

Category B Infringements

- Use of File sharing software e.g. Bitorrent etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible Sanctions: Removal within classroom from ICT equipment, Directorate detention, teacher/directorate contacts home, teacher to inform ICT team to invoke possible removal of Internet access rights for a period.

Category C Infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or instant message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions: Immediate remove, referral to ICT team with possible removal of Internet and/or ICT access rights for a period, Head of Year to contact parents.

Category D Infringements

- Continued sending of emails or instant messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the Academy name into disrepute

Possible Sanctions – Referred to Principal /involvement of relevant pastoral leader/ internal seclusion / exclusion / removal of equipment / involvement of Safe Schools Police Officer.

Staff

Inappropriate use of the Academy ICT arrangements by staff is defined in the Communications Policy and may be dealt with under the Academy Disciplinary Policy

Complaints

The ICT team will act as the first point of contact for any complaint. Complaints against staff will be referred to the Head of School. Complaints against students will be handled in accordance with Academy behaviour and child protection policies. With specific regard to cyber-bullying, the Academy will make clear that the use of the web, text messages, email, video or audio to bully another student of member of staff will not be tolerated. If a bullying incident, directed at a student, occurs using email or mobile phone technology either inside or outside of Academy time staff should

- Advise the child not to respond to the message
- Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the Academy's Safeguarding officer

The ICT team/Safeguarding Officer may decide to:

- Remove the device to a secure place to ensure that there is no further access
- Inform the sender's e-mail service provider
- Notify parents of the students involved
- Consider informing the police depending on the severity or repetitious nature of offence
- Involve the safe schools officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff, the Academy's ICT team will be informed who will:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate

Records of complaints will be maintained in line with Academy behavior management policies and staff disciplinary policies.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The Safeguarding team and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.