E-SAFETY AND COMPUTER USAGE POLICY

1. INTRODUCTION

This policy supports the aims of the School in educating children to explore their horizons in line with the e-world safely and setting up a safety net around them. This policy applies to all members of the school community, including staff, pupils, parents, and visitors.

2. RATIONALE

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to equip our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web- based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Cloud computing, such as Showbie, GoogleDrive, iCloud Drive and OneDrive
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- iPad Devices

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At St Nicholas', we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual.

The loss of sensitive information can result in media coverage, potentially damage the reputation of the School, and incur possible financial penalties This can make it more difficult for the School to use technology to benefit learners.

Everybody in the School has a shared responsibility to secure any personal data and sensitive information used in their day to day professional duties and even staff not directly involved in data handling are made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff and pupils), are inclusive of both fixed and mobile internet; technologies provided by the school; and technologies owned by pupils and staff, but brought onto school premises.

3. MONITORING

The School has appropriate filters and monitoring in place as part of our obligation to comply with Keeping Children Safe in Education (September 2018) and the Prevent Duty.

The School requires all users of the wireless network to log in using their school supplied credentials. The School monitors online activity and is able to identify individuals as part of this process. A reporting system is in place for Designated Safeguarding Lead (DSL) and the Senior Leadership Team (SLT) to monitor online activity and easily identify any areas of concern.

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If you are in doubt as to whether the individual requesting such access authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request. ICT authorised staff may monitor, intercept, access, inspect, record and disclose e- mails, instant
messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law, including serious conduct or welfare concerns, extremism and the protection of others.. This may be to confirm or obtain School business related information; to confirm or investigate compliance with

School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018 , or to prevent or detect crime.
ICT authorised staff may, without prior notice, access the e-mail, or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

4. BREACHES OF POLICY
4.1 Response to a Data breach
In the event of any data breach, this must be reported immediately to the Head.
A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands.
The School must generally report a data breach to the Information Commissioner's Office (ICO)

without undue delay and within 72 hours if it presents a risk to individuals. In addition, the School must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether there is a need to notify the ICO.
4.2 Response to a Breach of Policy
A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to School IT systems.
4.3 Incident Reporting

Any breach that may be a breach of personal data must be reported immediately, following the procedure in 4.1 and within the Data Protection Guidance for Staff.
Any attempted or successful security breaches; loss of equipment; unauthorised use or suspected misuse of ICT; or unauthorized attempts to access personal data must be immediately reported to the Head.
Additionally, all security breaches, lost/stolen equipment or data, virus notifications, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head.
All eSafety incidents involving either staff or pupils should be recorded on the eSafety incident log by the Head.
4.4 Complaints
Complaints and/or issues relating to eSafety should be made to The Headteacher.
Incidents should be logged and the School procedure for investigating an eSafety incident should be followed.
4.4 Inappropriate Material
All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Head, depending on the seriousness of the offence; investigation by a member of the SLT,

immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

Where the allegation(s) concern the Head the staff member should report the matter to the Proprietor.

5. INCLUSION

The School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the School's eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

6. ROLES AND RESPONSIBILITIES

As eSafety is an important aspect of strategic leadership within the School, the Headmaster and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named eSafety Officer is Mr M. Donaldson.

All members of the School community have been made aware of who holds this post. It is the role of the eSafety Officer to keep abreast of current issues and guidance through organisations such as the DfE, CEOP (Child Exploitation and Online Protection), NSPCC and Childnet.

This policy, supported by the School's computer usage agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the school policies listed in the introduction to this policy.

7. COMPUTER VIRUSES

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If your machine is not routinely connected to the school network, you must make provision for the regular installation of software updates and virus definitions.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the ICT department. They will advise you what actions to take and be responsible for advising others that need to know.

8. DATA SECURITY

8.1 Guidelines, Responsibility and Management of Data

The accessing and appropriate use of school data is something that the School takes very seriously. Staff have been issued with and are required to follow the E- Safety and Computer Usage Policy, the Data Protection Policy and the Data Protection Staff Guidance. It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information. Any individual member of staff who produces electronic documents that contain personal data are responsible for ensuring secure storage and/or disposal.

Personal data sent or received via email must only be downloaded via agreed channels to the designated storage area, for example MIS. Sensitive data must not be stored in any Cloud Based Service. Staff must not hold sensitive or personal data on any device or memory stick that may be transferred out of the school grounds, including personal devices. Should there be an imperative to take personal data off- site, this must be agreed with a Leadership Team member beforehand and either the data or the storage device upon which it resides must be encrypted using a strong encryption algorithm.

When accessing the MIS externally, staff are required to complete a second authentication phase.

iPad devices must be locked or switched off when away from desks/workstations.

Electronic files must be securely deleted and staff should manage their download files either by deleting the files once they have been viewed and are no longer needed or visiting their download folder once a month and deleting files no longer required.

The School password procedures, including the format of the password and frequency of changing passwords, must be followed by all staff.

All staff should log off or lock a computer that they are using before leaving it unattended.

8.2 Personal devices

No personal data should be stored on or downloaded to personal devices. This includes not viewing email attachments if the attachment must be downloaded in order to be viewed.

The School recognises that in certain circumstances some staff may need to use their personal device including phone, tablet, laptop or PC, for work purposes. In this instance staff must only do so if they have the following in place:

- The device has security settings in place with a password, passcode or fingerprint ID setting.
- The temporary download folder on any device used is checked for any documents that may have been downloaded when viewing and are deleted immediately.
- If a personal device is used to access the School email or network systems, the Head must be notified immediately if this device is lost or stolen so that passwords to school accounts can be changed without delay.

If, in exceptional circumstances, staff need to hold school personal data on a personal device this must only be with permission from the Head and it must be encrypted. Staff are also reminded that they must not use their personal email accounts or personal mobile phones to make contact with students of the School expect in circumstances where prior permission has been given by the Head, as per the School's Safeguarding (Child Protection and Staff Behaviour) Policy and
Social Media Policy.

9. STUDENT AND STAFF EDUCATION AND TRAINING

9.1 eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.
The School has a framework for teaching internet skills in ICT and computer science lessons, as well as during tutorial sessions.
Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modeling and activities.
Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline, NSPCC or CEOP report abuse button.
In PSHE, pupils cover the topic of staying safe online, including understanding the risks of talking to strangers online and recognising the danger signals when using chat rooms. Cyber-bullying is also explored in depth.
Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

9.2 eSafety Skills Development for Staff

New staff receive information on the school's ESafety and Computer Usage Policy and the Data Protection Staff Guidance as part of their induction.
All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community.
All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas.
Our staff receive regular information and training on eSafety issues and data protection in the form of INSET or operational staff training sessions from the eSafety Officer, Designated Safeguarding Lead, or a nominated person. Data protection training is also provided via online training.

10. SYSTEMS AND ACCESS

10.1 Guiding Principles and Regulations

All staff are responsible for any activity on school systems carried out under access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.
No member of staff should allow any unauthorised person to use school ICT facilities and services that have been provided to them.
Staff should use only their personal logons, account IDs and passwords and not allow them to be

used by anyone else.
Enforced password changes take place on an annual basis for all members of staff.
Screen displays should be kept out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
Staff should ensure they log off or lock their device before moving away from a computer during the normal working day to protect any personal, sensitive (special category), confidential or otherwise classified data and to prevent unauthorised access.
Staff should not introduce or propagate viruses knowingly.
It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998. This is particularly relevant when downloading images for use in School from search engines such as Google, Bing, Yahoo, etc. This is regulated by the UK Intellectual
Property Office (https://www.gov.uk/government/organisations/intellectual-property-office).

10.2 E-mail
The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international.
The School gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e- mails and avoids the risk of personal profile information being revealed. Staff must not use personal email addresses for school work and should refrain from using their school email account for personal business.
It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The School email account should be the account that is used for all school business.
Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

MIS must be used to generate any emails being sent to more than one pupil or parent. When sending any emails to personal email addresses, for example the email address of a parent, the email address must be entered into the 'Bcc' (blind carbon copy) email address line. Parent or any other personal email addresses must never be entered into the 'To' or 'Cc' of the address line.
All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Members of staff should make every effort to ensure that emails are genuine before opening attachments or clicking on links within emails. If they are in any doubt then members of staff should, where practical, contact the sender to confirm that the email is genuine, and under no circumstances open attachments or click links if the sender is not known to then and if they are not expecting to receive email from the sender.
All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
Staff must inform the Head if they receive an offensive e-mail.

Pupils are introduced to e-mail as part of the ICT Scheme of Work. However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

10.3 Internet Usage
The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable

resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet at St Nicholas' is logged and the logs are randomly but regularly monitored.

Whenever any inappropriate use is detected it will be followed up. The following are regulated by the UK Intellectual Property Office (https://www.gov.uk/government/organisations/intellectual-property-office) - Link. Raw image searches are discouraged when working with pupils.
All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience. Staff are advised to

be particularly cautious with the increased use of social media and retain a positive tone at all times, ensuring that the reputation of the school, its staff and governors are promoted and protected and that stakeholders understand their ambassadorial role with regards to Park Hill. Don't reveal names of colleagues, pupils or parents, or any other confidential information acquired through your job on any social networking site or blog.
On-line gambling is not allowed.
Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
The school does not allow pupils access to internet logs or blogs.
The school uses management control tools for controlling and monitoring workstations.
It is the responsibility of the school, by delegation to the network manager, to ensure that Anti- virus protection is installed and kept up-to-date on all school machines.
Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the School's responsibility nor the Head of ICT Services to install or maintain virus protection on personal systems.
Pupils and staff are not permitted to download programs on school based technologies without seeking prior permission from the Head.

11. PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION
All users should:
● Ensure that any School information accessed from your own PC or other media equipment is kept secure.
● Ensure you log off or lock the screen before moving away from your computer during your normal working day to prevent unauthorised access.
● Ensure the accuracy of any personal, sensitive, confidential and classified information.
● Do not share any pupil, parents or staff personal data with third parties unless there is a lawful reason to do so and/or a third party agreement is in place.
● Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
● Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print.
● Not to post on the Internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
● Keep the screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
● Ensure hard copies of data are securely stored and disposed of after use.Paper records containing personal data must be kept under lock and key. Records which contain sensitive or confidential information should be stored in a designated secure location with additional security. Sensitive/personal data held in paper form must be shredded via the external company process when no longer required. Any individual member of staff who produces any hard copy documents (including photocopying) that contain personal data are responsible for ensuring secure storage

and/or disposal. Electronic files must be securely deleted by the secure methods provided within the Data Protection Staff Guidance. Select the most appropriate storage medium and location for personal information and especially personal information of a sensitive nature. Sensitive (special category) data must not be stored in any Cloud Based Service.

Refrain from emailing personal information to their own personal email account and from sharing cloud based documents with their own personal cloud storage accounts.

13. SAFE USE OF IMAGES

Digital images are easy to capture, reproduce and publish and, therefore, misuse.

Digital images are easy to capture, reproduce and publish and, therefore, misuse. The Taking, Storing and Using Images Policy must be followed for the storing and use of images of pupils, staff or visitors.

14. ICT EQUIPMENT WITHIN SCHOOL

14.1 PCs and Other School Equipment

As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

It is imperative that you save your data on a frequent basis to the school's network drive, or store information with school provided cloud based service. You are responsible for the backup and restoration of any of your data that is not held either on the school's network drive or within a cloud based service provided by the school

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

All activities carried out on School systems and hardware will be monitored in accordance with the general policy.

Staff must ensure that all school data is either stored on school's network, or within a school provided clouds based service, and not kept solely on a laptop.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

Ensure portable and mobile ICT equipment is made available as necessary for anti- virus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by our ICT support.

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight. Portable equipment must be transported in its protective case if supplied.

14.2 Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, tablets, mobile and smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Permission must be sought before any image or sound recordings are made on these devices of any member of the School community.

The School is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any member of the School community is not allowed.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

The School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device unless it is for the purpose of enhancing their duties (eg contacting a student with information during a school trip).

Personal mobile telephones and cameras should not be used when members of staff are teaching or involved in an activity with the pupils. However, under exceptional cases, but not in EYFS, if a member of staff does not have a School camera and considers that a photograph/film of a child/

children would be beneficial for School purposes or to show a child's progress, they may use their own device. The photographs/film must be transferred to School equipment at the earliest opportunity and deleted from the member of staff's personal device immediately. Photos cannot be used or passed on outside the School. Neither staff nor children may use their own mobile phones to take photographs within our EYFS setting. Some digital cameras are available from the DDLT in CHICT.
The group leader on all trips and visits involving an overnight stay should take a School mobile phone with him/her and may ask the pupils for their mobile numbers before allowing them out in small, unsupervised groups. The School mobile should be used for any contact with pupils that may be necessary. The group leader will delete any record of pupils' mobile phone numbers at the end of the trip or visit and should ensure that pupils delete any staff numbers that they may have acquired during the trip.

The School allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device unless it is for the purpose of enhancing their duties (eg contacting a student with information during a school trip).

15.1 Staff
Upon leaving the employment of St Nicholas' School, members of staff shall have their Windows Domain and Management Information System (MIS) access withdrawn immediately.

16. CURRENT LEGISLATION

16.1 Acts Relating to Monitoring of Staff eMail
Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm
Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm
16.2 Other Acts Relating to eSafety and personal data
Racial and Religious Hatred Act 2006
Sexual Offences Act 2003
Communications Act 2003 (section 127)
The Computer Misuse Act 1990 (sections 1 – 3) Malicious Communications Act 1988 (section 1)

Copyright, Design and Patents Act 1988 Public Order Act 1986 (sections 17 – 29) Protection of Children Act 1978 (Section 1) Obscene Publications Act 1959 and 1964 Protection from Harassment Act 1997
Cloud Computing Services (2006)
https://www.gov.uk/government/publications/cloud-computing-how-schools-can- move-services- to-the-cloud

Policy reviewed by: M. Donaldson

Policy Sign Off - Mr. Amit Mehta, Chairman and Governor

Review date: September 2018

Next review date: September 2019