ST ALBANS GIRLS' SCHOOL

ONLINE SECURITY POLICY (Non-Statutory)		
GB sub-committee: Finance, Premises and Operations		
Co-ordinator: P O'Neill		
Last Reviewed: Summer 2020	**Next Review: Summer 2021**	

Signed by…………………………………………..
Margaret Chapman (Head Teacher)

Signed by………………………………………..
Claire Barnard (Chair of Governors)

1.	**RATIONALE**	
	1.1.1	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 arm our young people with the skills to access life-long learning and employment
	1.1.2	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 • Apps • E-mail, Instant Messaging and chat rooms • Social Media, including Facebook and Twitter • Mobile/ Smart phones with text, video and/ or web functionality • Other mobile devices including tablets and gaming devices • Online Games • Learning Platforms and Virtual Learning Environments • Blogs and Wikis • Podcasting • Video sharing • Downloading • On demand TV and video, movies and radio / Smart TVs
	1.1.3	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 and that some have minimum age requirements, usually 13 years. All web-based programmes suggested by the school to students will meet the required General Data Protection Regulations (GDPR), the school will maintain a record of such web based programmes
	1.1.4	Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors[for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies

		owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices)
1.2	**Acts Relating to Monitoring of Staff eMail**	
	1.2.1	Data Protection Act 1998
		At a glance: Data protection is about ensuring people can trust you to use their data fairly and responsibly. As we collect information about individuals for reasons other than our own personal, family or household purposes, we need to comply. The UK data protection regime is set out in the DPA 2018, along with the GDPR (which also forms part of UK law). It takes a flexible, risk-based approach which puts the onus on the school to think about and justify how and why we use data. The ICO regulates data protection in the UK. they offer advice and guidance, promote good practice, carry out audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate For more information see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
	1.2.2	**Regulation of Investigatory Powers Act 2000**
		Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. https://www.legislation.gov.uk/ukpga/2000/23/contents Human Rights Act 1998 https://www.legislation.gov.uk/ukpga/1998/42/schedule/1
1.3	**Other Acts Relating to eSafety**	
	1.3.1	Racial and Religious Hatred Act 2006 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.
	1.3.2	Sexual Offences Act 2003 The new 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. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document

		as part of their child protection packs
	1.3.3	Communications Act 2003 (section 127) 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
	1.3.4	The Computer Misuse Act 1990 (sections 1 – 3) Regardless of an individual's motivation, the Act makes it a criminal offence to gain: • access to computer files or software without permission (for example using another person's password to access files) • unauthorised access, as above, in order to commit a further criminal act (such as fraud) • impair the operation of a computer or program UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.
	1.3.5	Malicious Communications Act 1988 (section 1) This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety Copyright, Design and Patents Act 1988 Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.
	1.3.6	Public Order Act 1986 (sections 17 – 29) 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.
	1.3.7	Protection of Children Act 1978 (Section 1) 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.
	1.3.8	Obscene Publications Act 1959 and 1964

		Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.
	1.3.9	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.
	1.3.10	Counter-Terrorism and Security Act 2015 (Prevent), Anti-Radicalisation and Counter Extremism.
1.4	**Acts Relating to the Protection of Personal Data - Data Protection Act 2018**	
	http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted The Freedom of Information Act 2000 https://www.legislation.gov.uk/ukpga/2000/36/contents	
2.	**AIMS**	
2.1	To ensure the safety of all members of the school community when using ICT hardware and software	
2.2	To ensure that all confidential information is managed appropriately	
2.3	To provide guidance on acceptable use of ICT hardware and software	
2.4	To ensure compliance with national legislation as outlined within the policy	
2.5	To protect the ICT assets of the school	
2.6	To outline professional responsibilities in relation to the use of ICT hardware and software	
2.7	To clarify expectations in relation to use of ICT both within and outside the school environment	
3.	**PROCEDURE**	
3.1	**Computer Viruses**	
	3.1.1	Never interfere with any anti-virus software installed on school ICT equipment
	3.1.2	If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
	3.1.3	If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know
3.2	**Breaches of policy**	
	3.2.1	A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual
	3.2.2	For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated
	3.2.3	Policy breaches may also lead to criminal or civil proceedings
	3.2.4	The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act
	3.2.5	The data protection powers of the Information Commissioner's Office are to: • Conduct assessments to check organisations are complying with the Act; • Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

		• Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law; • Prosecute those who commit criminal offences under the Act; • Conduct audits to assess whether organisations' processing of personal data follows good practice, • Report to Parliament on data protection issues of concern For students, reference will be made to the school's behaviour policy as well as the Student Privacy Notice
3.3	**Incident Reporting**	
	3.3.1	Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Karen Thomas, Deputy Headteacher or David Adams, Trust Network Manager. Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements
3.4	**Disposal of redundant ICT equipment**	
	3.4.1	All redundant ICT equipment will be disposed of through an authorised agency, in accordance with redundant equipment disposal policy. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
	3.4.2	All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
	3.4.3	Disposal of any ICT equipment will conform to: • The Waste Electrical and Electronic Equipment Regulations 2006 • The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007 • http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e • Data Protection Act 2018 • https://ico.org.uk/for-organisations/in-your-sector/education/ • Electricity at Work Regulations 1989 https://www2.theiet.org/forums/forum/messageview.cfm?catid=205&threadid=12078
	3.4.4	The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
	3.4.5	The school's disposal record will include: • Date item disposed of • Authorisation for disposal, including: • verification of software licensing • any personal data likely to be held on the storage media? * • *if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed • How it was disposed of eg waste, gift, sale

		• Name of person & / or organisation who received the disposed item • Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate Further information available at: • **Waste Electrical and Electronic Equipment (WEEE) Regulations** • **Environment Agency web site** • Introduction • http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx • The Waste Electrical and Electronic Equipment Regulations 2006 http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf • The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007 http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e • **Information Commissioner website** https://ico.org.uk/ • **PC Disposal – SITSS Information** www.thegrid.org.uk/info/traded/sitss/services/computer_managment/PC_disposal/
3.5	**Email**	
	The use of e-mail within most schools is an essential means of communication for both staff and students. 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 student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and how to behave responsibly online	
	3.5.1	The school gives all staff their own e-mail account to use for all school business as a work-based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
	3.5.2	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
	3.5.3	Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses
	3.5.4	The school attaches a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
	3.5.5	All e-mails should be written and checked carefully before sending, with the same care given as with all external communication
	3.5.6	Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
	3.5.7	E-mails created or received as part of a school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
	3.5.8	All students have their own individual school issued accounts
	3.5.9	The forwarding of chain emails is not permitted in school
	3.5.10	All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour, 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
	3.5.11	Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail
	3.5.12	Staff must inform the Deputy Head if they receive an offensive e-mail

	3.5.13	Students are introduced to e-mail as part of the Computing Programme of Study
	3.5.14	However members of the school community access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply
	3.5.15	Staff should use their own school e-mail account so that they are clearly identified as the originator of a message
	3.5.16	Staff should keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
	3.5.19	Staff should not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
	3.5.20	School e-mail is not to be used for personal advertising.
	3.5.21	Staff should check their e-mail regularly.
	3.5.22	Staff should activate their 'out-of-office' notification when away for extended periods.
	3.5.23	Staff and students should never open attachments from an untrusted source; Consult the network manager first.
	3.5.24	Staff should not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
	3.5.25	The automatic forwarding and deletion of e-mails is not allowed.
3.6	**E-mailing personal, sensitive, confidential or classified information**	
	3.6.1	Where your conclusion is that e-mail must be used to transmit such data: • Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail: • Encrypt and password protect. See http://www.thegrid.org.uk/info/data protection/#securedata • Verify the details, including accurate e-mail address, of any intended recipient of the information • Verify (by phoning) the details of a requestor before responding to e-mail requests for information • Do not copy or forward the e-mail to any more recipients than is absolutely necessary • Do not send the information to any person whose details you have been unable to separately verify (usually by phone) • Send the information as an encrypted document **attached** to an e-mail • Provide the encryption key or password by a **separate** contact with the recipient(s) Do not identify such information in the subject line of any e-mail Request confirmation of safe receipt
3.9	**Esafety development skills for staff**	
	3.9.1	Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages.
	3.9.2	Details of the ongoing staff training programme can be found in the CPD evidence folder
	3.9.3	New staff receive information on the school's acceptable use policy as part of their induction.
	3.9.4	All staff have been made aware of their 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.
	3.9.5	All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

3.10	**Internet Access**	
	Infrastructure - procedures	
	3.10.1	Hertfordshire Local Authority has a monitoring solution via the Hertfordshire Grid for Learning where web-based activity is monitored and recorded
	3.10.2	School internet access is controlled through the HICS web filtering service. For further information relating to filtering please go to: http://www.thegrid.org.uk/eservices/safety/filtered.shtml
	3.10.3	St Albans Girls' School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
	3.10.4	Staff and students are aware that school based email and internet activity can be monitored and explored further if required
	3.10.5	The school does not allow students access to internet logs
	3.10.6	The school uses management control tools for controlling and monitoring workstations
	3.10.7	If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
	3.10.8	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
	3.10.9	Students 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. All external devices are automatically checked for viruses on connection with the school network
	3.10.10	Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the network manager
	3.10.11	If there are any issues related to viruses or anti-virus software, the network manager should be informed immediately.
3.11	**Managing Other Online Technologies**	
	3.11.1	Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.
	3.11.2	At present, the school endeavours to deny access to social networking and online games websites to students within school.
	3.11.3	Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Headteacher
	3.11.4	Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm
3.12	**Parental involvement**	
	3.12.1	We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.
	3.12.2	• Parents/carers and students are actively encouraged to contribute to adjustments or reviews of the school eSafety policy by contacting the school • Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

		• Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website) • Parents/carers are invited to an annual e-safety evening to provide updates on e-safety • Parents/carers are expected to sign a Home School agreement to enable their child to make use of school ICT systems • We will support the school approach to on-line safety and not deliberately upload or add any text, image, sound or videos that could upset or offend any member of the school community or bring the school name into disrepute. • The school disseminates information to parents relating to eSafety where appropriate in the form of; • Information evenings • Practical training sessions e.g. current eSafety issues • Posters • School website information • Newsletter items/passwords and password security procedures
3.13	**Passwords**	
	3.13.1	Please refer to the document on the grid for guidance on How to Encrypt Files, which contains guidance on creating strong passwords and password security **http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata**
	3.13.2	Always use your own personal passwords.
	3.13.3	Make sure you enter your personal passwords each time your logon. Do not include passwords in any automated logon procedures.
	3.13.4	Staff should change temporary passwords at first logon.
	3.13.5	Change passwords whenever there is any indication of possible system or password compromise.
	3.13.6	Change passwords whenever there is any indication of possible system or password compromise.
	3.13.7	Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.
	3.13.8	Never tell a child or colleague your password.
	3.13.9	If you aware of a breach of security with your password or account inform the Deputy Head immediately
	3.13.10	Passwords must contain a minimum of six characters and be difficult to guess
	3.13.11	Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
	3.13.12	User ID and passwords for staff and students who have left the school are removed from the system within **48 hours**
	3.13.13	If staff think their password may have been compromised or someone else has become aware of their password they should report this to the Network Manager
	3.13.14	All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
	3.13.15	Staff are provided with an individual network, email, VLE and SIMS log-in username. They are also expected to use a personal password and keep it private
	3.13.16	Students are not allowed to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others
	3.13.17	Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including

		ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked
	3.13.18	Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
	3.13.19	In our school, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times
3.14	**Zombie Accounts**	
	3.14.1	Zombie accounts refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access
	3.14.2	The network manager is to ensure that all user accounts are disabled once the member of the school has left
3.15	**Protecting personal, sensitive, confidential and classified information**	
	3.15.1	Staff should ensure that any school information accessed from their own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended
	3.15.2	Staff should ensure that they lock their screen before moving away from their computer during their normal working day to prevent unauthorised access
	3.15.3	Staff should ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share with others
	3.15.4	Staff should ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
	3.15.5	Staff should ensure that the security of any personal, sensitive, confidential and classified information contained in documents they fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.
	3.15.6	Staff should ensure that they only download personal data from systems if expressly authorised to do so by their manager.
	3.15.7	Staff must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
	3.15.8	Staff should ensure that they keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.
	3.15.9	Staff should ensure that hard copies of data are securely stored and disposed of after use in accordance with the document labelling.
	3.15.10	Staff should ensure that removable media is purchased with encryption.
	3.15.11	Staff should ensure that they store all removable media securely.
	3.15.12	Staff should ensure that they securely dispose of removable media that may hold personal data.
	3.15.13	Staff should ensure that they encrypt all files containing personal, sensitive, confidential or classified data.
	3.15.14	Please refer to the document on the grid for guidance on How to Encrypt Files.
	3.15.15	http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata.
3.16	**Remote Access procedures**	
	13.16.1	Staff are responsible for all activity via their remote access facility.
	13.16.2	Staff should only use equipment with an appropriate level of security for remote access.
	3.16.3	To prevent unauthorised access to school systems, staff should keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

	3.16.4	Staff should select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers.
	3.16.5	Staff should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
	3.16.6	Staff should protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.
3.17	**Taking of images and film**	
	3.17.2	With the consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment
	3.17.3	Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students; this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
3.18	**Publishing students' images and work**	
	3.18.1	On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:
		Staff should only use equipment with an appropriate level of security for remote access • on the school web site • in the school prospectus and other printed publications that the school may produce for promotional purposes • recorded/ transmitted on a video or webcam • in display material that may be used in the school's communal areas • in display material that may be used in external areas, ie exhibition promoting the school • general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically) • This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc • Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school • E-mail and postal addresses of students will not be published. Students' full names will not be published alongside their image, without student + parental permission • Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed • For further information relating to issues associated with school websites and the safe use of images in Hertfordshire schools, see http://www.thegrid.org.uk/schoolweb/safety/index.shtml http://www.thegrid.org.uk/info/csf/policies/index.shtml#images
3.19	**Storage of images**	
	3.19.1	Images/ films of children are stored on the school's network, website
	3.19.2	Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource
3.20	**Webcams and CCTV**	
	3.20.1	The school uses CCTV for security and safety. The only people with access to this are the site team and the Senior Leadership Team. Notification of CCTV use is displayed at the front of the school
	3.20.2	Webcams will not be used for broadcast on the internet without prior parental consent

	3.20.3	Misuse of any webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
	3.20.4	Consent is sought from parents/carers and staff on joining the school, in the same way as for all images
	3.20.5	Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices
3.21	**Video Conferencing**	
	3.21.1	Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
	3.21.2	All students are supervised by a member of staff when video conferencing.
	3.21.3	Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference
	3.21.4	For further information and guidance relating to Video Conferencing, please see: http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml
3.22	**School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media procedures**	
	School ICT Equipment – expectations of Users	
	3.22.1	As a user of the school ICT equipment, all users are responsible for their activity.
	3.22.2	The school logs ICT equipment issued to staff and record serial numbers as part of the school's inventory.
	3.22.3	Do not allow visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
	3.22.4	Ensure that all ICT equipment is kept physically secure.
	3.22.5	Users should 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.
	3.22.6	It is imperative that users save their data on a frequent basis to the school's network. Users are responsible for the backup and restoration of any data that is not held on the school's network.
	3.22.7	Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted.
	3.22.8	It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
	3.22.9	Privately owned ICT equipment should not be used on a school network without prior permission from the Network Manager.
	3.22.10	On termination of employment, resignation or transfer, users should return all ICT equipment to the Network Manager. They must also provide details of all system logons so that they can be disabled.
	3.22.11	It is the responsibility of users to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
	3.22.12	All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).
3.23	**Portable and Mobile ICT Equipment**	
	This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data	

	3.23.1	All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
	3.23.2	Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop or tablet. Any equipment where personal data is likely to be stored must be encrypted.
	3.23.3	Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, you must place the laptop in the boot of your car before starting your journey.
	3.23.4	Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.
	3.23.5	Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
	3.23.6	The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.
	3.23.7	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.
	3.23.8	Portable equipment must be transported in its protective case if supplied.
	3.23.9	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 student or parent/carer using their personal device.
	3.23.10	Students are allowed to bring personal mobile devices/phones to school but must keep them in their lockers throughout the day. At all times the device must be switched onto silent.
	3.23.11	The school is not responsible for the loss, damage or theft of any personal mobile device
	3.23.12	The sending of inappropriate text messages between any member of the school community is not allowed and will be managed using the school's behaviour policy and/or disciplinary procedures.
	3.23.13	Permission must be sought before any image or sound recordings are made on these devices by any member of the school community.
	3.23.14	Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
	3.23.15	Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
	3.23.16	Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
3.24	**Servers**	
	3.24.1	Servers are kept in a locked and secure environment.
	3.24.2	Access rights to servers are limited.
	3.24.3	Servers are password protected and locked.
	3.24.4	Existing servers have security software installed appropriate to the machine's specification.
	3.24.5	Data is backed-up regularly.
	3.24.6	Back-up media stored off-site is secure.
	3.24.7	Remote back-ups are automatically securely encrypted. SITSS provide an encrypted remote back up service. Please contact the SITSS helpdesk for further information – 01438 844777.
3.25	**Social Media, including Facebook and Twitter**	
	3.25.1	Our school uses Facebook and Twitter to communicate with parents and carers. The authorised staff are responsible for all postings on these technologies and monitors responses from others.

	3.25.2	Staff are not permitted to access their personal social media accounts using school equipment.
	3.25.3	Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach students the safe and responsible use of Social Media.
	3.25.4	Students are not permitted to access their social media accounts whilst at school.
	3.25.5	Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
	3.25.6	Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
	3.25.7	Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law.
3.26	**Telephone Services Procedures**	
	3.26.1	• Staff may make or receive personal telephone calls provided: • They are infrequent, kept as brief as possible and do not cause annoyance to others • They are not for profit or to premium rate services • They conform to this and other relevant HCC and school policies.
	3.26.2	School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
	3.26.3	Staff should be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
	3.26.4	Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office.
	Staff and Student Involvement in Policy Creation	
	Staff, governors and students have been involved in making/ reviewing the Policy for ICT Acceptable Use through staff meetings, assemblies, information evenings and via the VLE.	
4.	**MONITORING**	
4.1	There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them.	
4.2	This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.	
4.3	**The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.**	
4.4	This policy has been read, amended and approved by the staff, head teacher and governors.	
4.5	As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Karen Thomas who has been designated this role as Deputy Headteacher. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as Herts LA, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.	
4.6	Senior Management and governors are updated by the Head/ eSafety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.	
4.7	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 is	

	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.
4.8	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.
4.9	All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful.

ST ALBANS GIRLS' SCHOOL

Equality Impact Analysis

When reviewing all schools' policies, the following Equality Impact Analysis (EIA) should be undertaken to ensure fairness of the new proposals/policy and to identify any action needed to redress any potential discrimination, positively promoting equal opportunities, improved access and participation for all.

Title of Policy:	On-Line Security	
Date:	Summer 2020	
EIA carried out by:	Mr Phil O'Neill	
EIA reviewed by:	Personnel & Student Wellbeing Committee	

1. Identify the aims and objectives of the policy, what will be the proposed change and how will it be implemented	
• **Policy contains information about:** Overall aims and objectives? What is the proposed change? Who is intended to benefit from the proposal and in what way? Outcomes of the policy? How will it be put into practice and who is responsible for this?	To ensure the safety of all members of the school community when using ICT hardware and software To ensure that all confidential information is managed appropriately To provide guidance on acceptable use of ICT hardware and software To ensure compliance with national legislation as outlined within the policy To protect the ICT assets of the school To outline professional responsibilities in relation to the use of ICT hardware and software To clarify expectations in relation to use of ICT both within and outside the school environment

2. Assessment of Impact? *To include impact of policy, any plans needed to mitigate any negative impact, equality issues to be addressed*		
Characteristic	Group	Effect/Impact
• Age		No impact
• Disability		No impact
• Gender reassignment		No impact
• Marriage/civil partnership		No impact
• Pregnancy/Maternity		No impact
• Race		No impact
• Religion or Belief		No impact
• Sex		No impact
• Sexual orientation		No impact

3. Consultation	
• **New policy contains information about:** Policy audience, expected actions and outcomes. Consultation and communication process Accessibility for all Fair access to the consultation process Lessons learnt from previous consultation, if appropriate	Expectations, requirements and actions

4. Decision	
• Should the new proposal/policy be agreed and any impacts identified following consultations? • What reasonable adjustments are required?	No issues or adjustments required

5. Action Planning	
• Any actions identified to address inequality for different groups? • Any actions identified to promote equality and diversity? • Where are these actions recorded and who is responsible for them?	None

6. Monitoring and Review	
• When will the impact assessment be reviewed? • Who is responsible?	Summer 2021, in line with policy Phil O'Neill

7. Publication of the results of the impact assessment	
• Results of EIA are published – where and when? • The results are kept as a public record of the EIA – where and when?	With policy