	ST ALBANS GIRLS' SCHOOL
Online Safety Policy	
GB sub-committee: Personnel & Student Wellbeing Committee	
Co-ordinator: Miss T Lambert & Mrs P Jarvis	
Last Reviewed: Summer 2024	**Next Review: Summer 2025**
	
Signed by: **Margaret Chapman** ***Head Teacher***	**Signed by:** **Claire Barnard** ***Chair of Governors***

1. RATIONALE	
1.1	Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: ● A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited ● Key online safety messages should be reinforced as part of a planned programme of assemblies and form time activities ● Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information. ● Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet ● Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making in line with the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. ● Students will be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. ● Staff should act as good role models in their use of digital technologies, the internet and mobile devices ● Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. ● It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that

	the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
1.2	This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on: ● Teaching online safety in schools ● Preventing and tackling bullying and cyber-bullying: advice for head teachers and school staff ● Relationships and sex education ● Searching, screening and confiscation ● Online Sexual Harassment including the sending of Nudes and Semi Nudes 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, the PSHE Association recommended programmes of study and Education for a Connected World Guidance.
2. AIMS	
2.1	The purpose of STAGS' online safety policy is to: ● Safeguard and protect all members of the St Albans Girls' School community online. ● Identify approaches to educate and raise awareness of online safety throughout the community. ● Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology. ● Identify clear procedures to use when responding to online safety concerns. STAGS identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk: ● Content: being exposed to illegal, inappropriate or harmful material ● Contact: being subjected to harmful online interaction with other users ● Conduct: personal online behaviour that increases the likelihood of, or causes, harm. ● Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. 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.
3. PROCEDURES	
Roles and Responsibilities for Online Safety	
3.1	**The Governing Body and Governor responsible for Online Safety** Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Personnel, Student Wellbeing Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body, Mrs Amanda Jefferies has taken on the role of Online Safety Governor who is also the Governor responsible for Safeguarding The role of the Online Safety Governor will include: ● regular meetings with the Designated Senior Lead for Safeguarding; ● regular monitoring of online safety incident logs; ● regular monitoring of filtering/change control logs; ● reporting to relevant Governors meetings.
3.2	**The Head Teacher** The Head Teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
3.3	**Designated Safeguarding Lead** Details of the school's DSL, Ms Tessa Lambert, Deputy Head Teacher and Deputy DSL Miss Tamsin Holland, Assistant Head Teacher: Key Stage 3 are set out in our child protection and safeguarding policy as well relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular: ● Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school; ● Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents; ● Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy; ● Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy; ● Updating and delivering staff training on online safety (appendix 5) contains a self-audit for staff on online safety training needs); ● Liaising with other agencies and/or external services if necessary; ● Providing regular reports on online safety in school to the head teacher and/or governing board; This list is not intended to be exhaustive.
3.4	**The Trust Network Manager** The Trust Network Manager, Mr Nick Clarke is responsible for: ● Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;

	● Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly; ● Conducting a full security check and monitoring the school's ICT systems on a regular basis; ● Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files; ● Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy ● Ensuring that any incidents of cyber-bullying are reported to ensure that they are dealt with appropriately in line with the school behaviour policy. This list is not intended to be exhaustive.
3.5	**All Staff, including temporary staff and volunteers** All staff, including contractors, agency staff, and volunteers are responsible for: ● Maintaining an understanding of this policy; ● Implementing this policy consistently; ● Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2a), and ensuring that students follow the school's terms on acceptable use (appendix 1); ● Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy and the school's Safeguarding Policy; ● Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy. This list is not intended to be exhaustive.
3.6	**All students (including consortium students)** All students, including those who attend consortium lessons are responsible for: ● using the school's digital technology systems in accordance with the student acceptable use agreement (appendix 1); ● following the school's Blended Learning Policy when using a personal device in lessons; ● have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations; ● need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so; ● will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying; ● should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
3.7	**Role of Parents** Parents are expected to: ● Notify a member of staff or the Head Teacher 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 (appendix 1);

	● For safeguarding reasons parents/carers are advised to not use camera phones to take images on school grounds; ● Not place images of other children taken at school on social media sites without the consent from the parents involved; ● Report if their child has been or is witness to online sexual harassment to the school and/or police; ● Parents can seek further guidance on keeping children safe online from the following organisations and websites: ○ What are the issues? - UK Safer Internet Centre ○ Hot topics - Childnet International ○ Parent fact sheet - Childnet International ○ Parent guides and online safety information - Smoothwall Online Safety Hub ○ Reporting an online concern - CEOP
Educating about Online Safety	
3.8	**Students** will be taught about online safety as part of the curriculum. In line with the National Curriculum for Computing and the Statutory Duty to teach Relationships and Sex Education students will be able to: In **Key Stage 3**: ● 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. In **Key Stage 4**: ● To understand how changes in technology affect safety, including new ways to protect their online privacy and identity; ● How they report a range of concerns. Additionally, by the **end of secondary school**, they will know: ● Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online; ● About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online; ● Not to provide material to others that they would not want shared further and not to share personal material which is sent to them; ● What to do and where to get support to report material or manage issues online; ● The impact of viewing harmful content; ● That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners; ● That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail; ● How information and data is generated, collected, shared and used online; ● How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

	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 students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this when appropriate to do so.
3.9	**Parents** Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through: ● Letters and Newsletters; ● School website; ● Parents/Carers information evenings; ● High profile events/campaigns e.g. Safer Internet Day.
Cyber-Bullying	
3.10	Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that has taken place out of school (See also the school behaviour policy and anti-bullying policy).
3.11	To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. ● We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. ● Teachers will discuss cyber-bullying with their form groups, and the issue will be addressed in assemblies. ● Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE and other subjects where appropriate. ● All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

	● The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
Examining Electronic Devices	
3.12	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 DSL 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.
3.13	**Smoothwall: Filtering and Monitoring** In line with KCSIE 2023 schools and colleges need to provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material. The DSL is responsible for this in liaison with the governing body. The school uses the filtering and monitoring system Smoothwall as an external provider to ensure that all devices and online activities used by the school community are monitored. The monitoring sits on devices and alerts are sent to the DSL 365 Days a year 24/7. Smoothwall reports instantly any safeguarding concerns via an email alert system or via phone call to the main school officer or DSL depending on risk. Filtering and monitoring reports are provided and accessible at all times from Smoothwall. Only DSL trained staff can access the system and act on alerts. The school also uses Smoothwall's Online Safety Hub (OSH) service. The purpose is to educate and support parents in navigating their children's digital safety and wellbeing and encourage uptake of both the OSH and the Qustodio app.
Acceptable Use Agreement	
3.14	All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1,

	2a and 2b). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1, 2a and 2b. If students do not comply with the acceptable use agreement sanctions will be decided upon following appendix 4 Flowcharts for Managing an Online Safety Incident and the school's behaviour policy.
Use of Mobiles in School	
3.15	This guidance outlines the appropriate use of mobile phones on our school site, school buses and on school trips/ activities. Students and parents/carers must read and understand the guidance below as a condition upon which permission is given to bring mobile phones to school. The Staff and Governors of STAGS recognise that many students and their families own a mobile phone. We also recognise that some parents/carers request that their child brings a mobile phone to school for safety and security reasons on the way to and from school. The school recognises that personal communication through mobile technologies is an accepted part of everyday adult life but that such technologies need to be used well. Our core business of teaching and learning needs to be conducted in an environment free from unnecessary distractions or disruptions.
3.16	Guidance on the use of mobile phones and Smartwatches ● It is the responsibility of students who bring mobile phones and smartwatches to school to abide by the guidelines outlined in this document ● It is incumbent upon parents to understand the capabilities and applications available on their child's phone and/or smartwatch ● In general, students should not bring valuable items to school, as they can be easily lost or stolen. Parents and carers should be aware if their child takes a mobile phone and/or smartwatch to school; it is assumed household insurance will provide the required cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to usage at school ● Students do not need to use mobile phones or access applications other than the time via their smartwatch during the school day. Parents and carers are reminded that in cases of emergency, the school office remains the point of contact and can ensure your child is reached quickly and assisted in any relevant way ● If mobile phones and/or smartwatches are brought into school by students, they should not be used between the hours of 8.35am and 3.10pm (apart from the time function on a smartwatch). This includes both break and lunchtime. Mobile phones should be switched off and kept locked (using a padlock) in students' lockers during the day ● It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their mobile phones or smartwatches (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords must not be shared ● Students must not use their mobile phone as an internet 'hotspot' for any reason ● The procedures applying to the inappropriate use and security of mobile phones, apply equally to the inappropriate use of Blended Learning devices

	● Sixth Form students are only permitted to use their mobile phone or smartwatches in the Sixth Form Centre (unless otherwise directed by subject teachers to enhance classroom learning ● It is forbidden for students to use their mobile phones to take videos and/or pictures of acts to denigrate and humiliate another student, and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student or member of staff without their consent. Mobile phones are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to fellow students, staff or visitors to the school. All online safety guidelines can be reviewed in the Online Safety Policy ● In order to avoid the accidental photographing of students, students are not permitted to take photographs of other students (including selfies) whilst on the school site, school activities or on school buses ● Mobile phones and watches are banned from all examinations ● The school's Behaviour Policy outlines the sanctions that will be imposed should expectations not be met in accordance with this guidance ● For safeguarding reasons, parents and carers must not take or record images on the school grounds
3.17	**Inappropriate Use of a Mobile Phone** Generally, a mobile phone will be deemed to have been used inappropriately if it; disrupts or is likely to disrupt the learning environment or interfere with the operation of the school day, threatens or is likely to threaten the safety or well-being of any person or is used illegally. ● Using mobile phones to bully and threaten other students is unacceptable. Cyber-bullying will not be tolerated. In some cases it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given; ● It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced; ● It is forbidden for students to use their mobile phones to take videos and/or pictures of acts to denigrate and humiliate another student/ staff member, and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile phones to photograph or film any student or member of staff without their consent. Mobile phones are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to fellow students, staff or visitors to the school; ● It is illegal to photograph another person without their consent. Students who do this must accept that there are legal consequences for this; ● In order to avoid the accidental photographing of students, students are not permitted to take photographs of other students (including selfies) whilst on the school site, school activities or buses, on route to and from school; ● Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence; ● Mobile phones and all other electronic devices are banned from all examinations. Students MUST hand all phones and electronic devices to invigilators before entering the exam hall. The examination boards have a zero tolerance policy if students are found in possession of mobile phones or electronic devices in the

	examination hall. The school will notify the examination board if any student is found in possession of a mobile phone during an examination.
3.18	**Sanctions for the misuse of mobile phones** ● If mobile phones are seen or heard during the school day they will be confiscated and a C4 issued in line with the school behaviour policy; ● It is unacceptable to take a picture of any student or member of staff without their permission. It is unacceptable to post any picture of a member of staff on the internet/ social media without permission of that person. In the event that this happens the student will be sanctioned and asked, and expected, to delete those images; ● The school reserves the right to take action if a student is involved in an incident of inappropriate behaviour, when a student is out of school and where they involve membership of the school community (e.g. cyber-bullying, use of images or personal information); ● In the event that an investigation into an incident is needed the school will expect students to co-operate and allow their phone to be accessed. A failure to cooperate will be considered an obstruction of justice; ● In addition to sanctions in school, actions involving the misuse of mobile phones could result in police intervention.
Use of Email	
3.19	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 email in relation to their age and how to behave responsibly online. As such: ● The school gives all staff their own email 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 emails and avoids the risk of personal profile information being revealed; ● 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 students, parents or conduct any school business using personal email addresses; ● The school attaches a standard disclaimer to be attached to all email 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; ● All e-mails should be written and checked carefully before sending, with the same care given as with all external communication; ● Students may only use school approved email accounts on the school system and only under direct teacher supervision for educational purposes ● 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; ● All students have their own individual school issued accounts; ● The forwarding of chain emails is not permitted in school;

	● All student email 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; ● Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail; ● Staff must inform the Deputy Head if they receive an offensive email; ● Students are introduced to email as part of the Computing Programme of Study; ● However, the members of the school community choose to access their school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply; ● Staff should use their own school email account so that they are clearly identified as the originator of a message; ● Staff should keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate; ● Staff should not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments; ● School email is not to be used for personal advertising; ● Staff should check their email regularly, but are not required to check email after 6pm Monday- Friday. Staff should aim to respond to all emails within 2 working days; ● Staff should activate their 'out-of-office' notification when away for extended periods; ● Staff and students should never open attachments from an untrusted source; Consult the network manager first; ● Staff should not use e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder; ● The automatic forwarding and deletion of e-mails is not allowed.
Staff using work devices outside of school	
3.20	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, as set out in appendix 2a. 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 containing data relating to the school must be encrypted. When accessing the school's MIS system outside of school, staff must use a two-factor authenticator to ensure cyber security. If staff have any concerns over the security of their device, they must seek advice from the Trust Network Manager. Work devices must be used solely for work activities.
Students using school devices outside of school	
3.21	On occasions it might be appropriate for the school to loan students an electronic device to enable them to work outside of school. Students using a school owned 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, as set out in appendix 1. If students have any concerns over the security of their device, they must seek advice from the Trust Network Manager. School devices must be used solely for school work activities.

Online Learning during school closure	
3.22	During an extended period of school closure during term time, learning will be provided in an online format. Online learning will also be provided from the second day of closure caused by inclement weather. Work will be provided to students via MIS System and Google Classroom. Google Meet sessions might also be provided to enable face-to-face learning to take place. During Google Meet sessions, all normal safeguarding procedures must be met by staff. See the Remote Learning Policy for more information about the school's policy and procedure for remote online learning.
Internet Access	
3.23	The internet is an open worldwide communication medium, available to everyone, 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 internet use through the HICS network (Hertfordshire Internet Connectivity Service) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up. Role of the internet within the school is set out below. ● The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity; ● Staff will preview any recommended sites, online services, software and apps before use; ● Searching for images through open search engines is strongly discouraged when working with students; ● If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research. It is recommended that links for such work are placed on Google Classroom; ● 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; ● Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience; ● Staff should not reveal names of colleagues, students, others or any other confidential information acquired through their job on any social networking site or other online application; ● On-line gambling or gaming is not allowed; ● It is at the Head Teacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.
Use of Social Media	
3.24	Our school uses Facebook, Twitter, LinkedIn and Instagram to communicate with parents and carers. The authorised staff are responsible for all postings on these technologies and monitor responses from others. Additionally:

	● Staff are not permitted to access their personal social media accounts using school equipment; ● Staff are able to set up 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; ● Students are not permitted to access their social media accounts whilst at school; ● 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; ● 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; ● Staff, governors, students, parents and carers are aware that their online behaviour should at all times be compatible with UK law. Services such as Facebook and Instagram have a 13+ age rating which should not be ignored
3.25	**Use of AI**
	Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Google Bard etc. St Albans Girls' School recognises that AI has many uses to help pupils learn, but may also lend itself to cheating and plagiarism. Pupils may use AI tools: As a research tool to help them find out about new topics and ideas when specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed. Pupils may not use AI tools: During assessments, including internal and external assessments and coursework to write their homework or class assignments, where AI-generated text is presented as their own work. St Albans Girls' School considers any unattributed use of AI-generated text or imagery to be plagiarism, and will follow our plagiarism procedures as set out in the Malpractice in Exams & Assessments Procedure.
Use of Digital and Video Images	
3.26	The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: ● When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of

	images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites; ● Ensure that written permission from parents or carers has been obtained before photographs of students are published on the school website/social media/local press ● In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images; ● Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes; ● Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute; ● Students must not take, use, share, publish or distribute images of others without their permission; ● Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images; ● Students' full names will not be used anywhere on a website or blog, particularly in association with photographs; ● Student's work can only be published with the permission of the student and parents or carers.
Video Conferencing	
3.27	Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school. If a student(s) is involved in a video conference, then: ● All students are supervised by a member of staff when video conferencing. This is either by the member of staff being in the room with the students or by attending the conference as well; ● The school keeps a record of video conferences, including date, time and participants; ● Approval from the Head Teacher is sought prior to all video conferences within school to end-points beyond the school; ● The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences; ● No part of any video conference is recorded in any medium without the written consent of those taking part; ● Parents are aware that some participants in conferences offered by 3rd party organisations may not be DBS checked; ● 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;

	For further information and guidance relating to Video Conferencing, please see: http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml
Data Protection	
3.28	Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. For information on what data is recorded, processed and transferred please refer to the Data Protection Policy and GDPR Policy.
Staff Training	
3.29	All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying, online sexual harassment and the risks of online radicalisation. An audit of needs is available in appendix 5. 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 DSL and Deputy DSL 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.
Dealing with unsuitable/inappropriate activities	
3.30	The school believes that the activities referred to in the following section would be inappropriate in a school context and that users must not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows: ● Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: ○ Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978; ○ Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003; ○ Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008; ○ Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986; ○ Pornography;

	○ Promotion of any kind of discrimination; ○ threatening behaviour, including promotion of physical violence or mental harm; ○ Promotion of extremism or terrorism; ○ Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute; ● Activities that might be classed as cyber-crime under the Computer Misuse Act: ○ Gaining unauthorised access to school networks, data and files, through the use of computers/devices; ○ Creating or propagating computer viruses or other harmful files; ○ Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords); ○ Disable/Impair/Disrupt network functionality through the use of computers/devices; ○ Using penetration testing equipment (without relevant permission); ● Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy; ● Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords); ● Unfair usage (downloading/uploading large files that hinders others in their use of the internet); ● Using school systems to run a private business; ● Online gambling; ● Online gaming (non-educational). ● If the school has evidence that a student or staff member has participated in unsuitable or inappropriate online activities the school will follow the Behaviour Policy for incidents involving students and the Staff Code of Conduct Policy for incidents involving a member of staff; ● For incidents involving parents the Head Teacher retains the right to restrict their access to the school, the school's IT systems and if deemed necessary to report the behaviour to the police.
Online Sexual Harassment	
3.31	The school defines Online Sexual Harassment to be: ● unwanted sexual behaviour on any digital platform. It can happen between anyone online, but this policy specifically focuses on students as victims and child on child incidences; ● Online sexual harassment can include a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different online platforms (private or public); ● Online platforms include (this is not an exhaustive list): ○ Social networking services: TikTok, Instagram, Snapchat, Facebook, Twitter; ○ Communication and messaging services: WhatsApp, Kik, iMessage, Facebook Messenger, Skype, Google Hangouts, Facetime; ○ Entertainment and gaming services: YouTube, Xbox Live, Playstation Network; ● It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against.

Dealing with Online Sexual Harassment	
3.32	Please also see the Safeguarding Policy. ● If a member of staff suspects that a child is the direct victim of online sexual harassment or a witness to online sexual harassment this must be reported immediately to the DSL or Deputy DSL; ● Staff should avoid viewing and must not download or store any images, messages or other files relating to the disclosure of online sexual harassment; ● The DSL or Deputy DSL should also avoid viewing files and instead should contact the police who can view such items if they are present on the students' personal device or a school device; ● The DSL or Deputy DSL must report the incident to the parents/carers, unless there is a safeguarding concern; ● The DSL or Deputy DSL will inform parents/carers that they must not share the image with them, but instead contact the police who are the only service allowed to access the image; ● The school supports Outcome 21 guidance which protects staff, parents and students who have unwittingly seen or shared youth produced sexual imagery (sexting); ● The school is aware that children can make mistakes including the creation of youth produced sexual imagery and the sharing of this imagery. Following the schools' Safeguarding Policy and Procedures, the DSL along with the Head Teacher reserve the right to not report the incident to Children's Service, the NSPCC or the Police if the child is not seen to be in immediate harm; ● If the incident is not reported to the police, following the schools' Safeguarding Policy the DSL or Deputy DSL will keep a written record of the incident. This record may be part of future Child Protection investigations carried out by Children's Services, the Police or the NSPCC; ● Even if the student, parent/carer do not want to escalate the situation to involve the police online sexual harassment must be reported to the police if it: ○ Involves coercion, blackmail or exploitation; ○ Are extreme or violent in their nature; ○ Involve a child or children under 13; ○ Involve a child at significant or immediate risk of harm; ○ Involve a child who is already recognised as vulnerable by children's social care or the police; ○ Involve images or recording of a crime, e.g a recording of an assault; ○ Involve more than one child; ● When the DSL or Deputy DSL is reporting Online Sexual Harassment to the police the Head Teacher must be informed and Online Safety Governor should be informed that a report has been made.
4. MONITORING	
4.1	The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3. This policy will be monitored every two years by the Senior Leadership Team and Governors to ensure that all employees comply with their professional requirements and procedures are appropriately adopted as required.

Appendix 1

Online Safety Policy - Acceptable Use Agreement: Students (2024)

- I will only use STAGS ICT systems in school, including the internet, e-mail, digital video, Chromebooks and mobile technologies for school purposes;
- When at school I will only use the school Wi-Fi to access the internet when using any type of personal device including a mobile phone;
- I will not download or install software on school technologies;
- I will only log onto the school network, other systems and resources with my provided personal username and password;
- I will always check files brought in on removable media (such as CDs, and USB drives etc.) with antivirus software and only use them if they are found to be clean of viruses;
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly;
- I will only use my school email account when contacting members of staff or for educational purposes;
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible;
- During a snow day or period of remote learning, when attending online lessons provided via Google Meet, I will ensure that I have protected my privacy by using a blank wall as my background, that I am appropriately dressed and any parents/carers or other family members in the room do not disrupt the learning taking place;
- I will be responsible for my behaviour when using the internet including my attendance at any online lessons provided via Google Meet. This includes resources I access and the language I use;
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher;
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher;
- I will not record images/footage of other students or staff at school - or during enrichment - unless requested to do so by a member of staff for a project or NEA assignment
- I will ensure that my online activity, both in school and outside school, will not cause the school, staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts;
- I will respect the privacy and ownership of others' work online at all times. I will respect copyright and intellectual property rights;
- I will not attempt to bypass the internet filtering system;
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers;
- If I bring a mobile phone and/or smartwatch to school, I am aware that I am responsible for it, and that it must be locked in my locker from 08:35 am – 3.10pm; smartwatches must only be used for their time function during the school day;
- If my year group is part of the blended learning programme, I will make sure that I follow the blended learning guidance including only using my device when directed to by teachers;
- I will not sign up to online services until I am old enough to do so; I will not access - or upload content to - any social media forum at school (including TikTok, Instagram etc.)
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents/carer may be contacted.

Student Signature…….

Parent/ Carer Signature ……

Form …….. Date ……

St Albans Girls' School

Learning for Life in a Community where All can Excel

Dear Parent/ Carer

ICT including the internet, e-mail, mobile technologies and online resources have become part of daily life. It is essential that students are aware of online safety and know how to stay safe when using any form of ICT.

At STAGS we encourage the positive use of ICT across the curriculum. To enable this to be a positive element of your child's education you will find attached our Acceptable Use of ICT Agreement. Students are expected to read and discuss this agreement with their parent/carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with Ms Tessa Lambert, Deputy Head Teacher.

Please return the bottom section of this form which will be kept on record at the school

---

Parent / carer signature

We have discussed this document with……. (child name) and we agree to follow the online safety rules and to support the safe use of ICT at St Albans Girls' School.

Parent/ Carer Signature …….

Student Signature……

Form …… Date ……

Appendix 2a – Online Safety Policy

Staff Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher.

- I will only use the school's ICT Systems and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher or Governing Body;
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities;
- I will ensure that all electronic communications with students and staff are compatible with my professional role;
- I will not give out my own personal details, such as mobile phone number, personal email address, or any other social media link, to students;
- I will only use the approved, secure email system(s) for any school business;
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely;
- I will use two factor authentication to ensure my access to MIS information remotely is secure;
- I will not install any hardware or software onto school ICT equipment, without permission of the Head Teacher;
- I will always check files brought in on removable media (such as CDs, and USB drives etc.) with antivirus software and only use them if they are found to be clean of viruses;
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;
- Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member;
- Images will not be distributed outside the school network - including the school's social media accounts - without the permission of the parent/carer, member of staff or Head Teacher;
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset or offend any member of the school community;
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher;
- I will respect copyright and intellectual property rights;
- If I am made aware of inappropriate content being on a students' device or mobile phone, I will immediately consult a member of the Safeguarding Team;
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation or that of others into disrepute;
- I will support and promote the school's Online Safety, GDPR and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies; I understand this forms part of the terms and conditions set out in my contract of employment;

- I will not use personal electronic devices in public areas of the school, except in the staff room or privacy of an office;
- I will keep school owned equipment physically secure in accordance with this policy. E.g. when travelling by car, I will place the laptop in the boot of my car before starting my journey as opposed to leaving it on display;
- I will ensure that all settings for personal social media accounts are set to private; I will make sure that I cannot be tagged on accounts visible by students;
- I will not upload comments or content about the school or Trust on my social media;
- I will not attempt to bypass the internet filtering system;
- I will pass onto the Safeguarding Team the details of any student or colleague that are not adhering to Online Safety Guidance (as per Appendices 1, 2a & 2b of the Online Safety Policy)

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature:
……

Full Name (printed):
……

Job Title:
……

Date:
……

Appendix 2b – Online Safety Policy
Governor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life. This user agreement/code of conduct is designed to ensure that all governors are aware of their responsibilities when using any form of ICT supplied by the school. All governors using ICT are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher.

- I will comply with the following rules when using and in relation to ICT equipment issued by the school:
- I will comply with the school ICT system security and not disclose any passwords provided to me by the school or other related authorities;
- I will ensure that all electronic communications with students and staff are appropriate and at all times, professional;
- I will not give out my own personal details, such as mobile phone number, personal email address, or any other social media link, to students;
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately;
- I will not install any hardware or software onto school ICT equipment;
- I will not browse, download, upload or distribute any material using the school's ICT that could be considered offensive, illegal or discriminatory;
- Images of students and/or staff will only be taken, stored and used for purposes in accordance with my responsibilities as a governor and in line with school policy and with written consent of the parent, carer or staff member;
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher;
- I will support the school approach to online safety;
- I understand that all my use of the Internet using the school's ICT systems and other related technologies belonging to the school can be monitored and logged. I will respect copyright and intellectual property rights;
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation as a governor or that of others into disrepute;
- As appropriate, I will support and promote the school's e-Safety and Data Protection policies and help students to be safe and responsible in their use of ICT and related technologies;
- I will not use personal electronic devices (including smart watches) in public areas of the school, except out of school hours or during governing body meetings, if appropriate;
- If school equipment is loaned, I will keep it physically secure.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature: ……

Full Name (printed): ……

Role: ……

Date: ……