Online Safety Policy

Our vision is to provide students with the confidence, skills and ambition to achieve a successful and productive life. We aim to ensure they leave us with the opportunities and are able to become positive members of their communities.

To do this, we have 3 principles that underpin our policies, practices and everything we do:

▪Everyone can learn, achieve and has the potential to be successful
▪Positive relationships are key to success and are underpinned by mutual trust, respect and caring for one another
▪We have high expectations in everything we do

INTRODUCTION

Seva Independent School (SIS) has a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity by:

▪ Discussing, reminding or raising relevant online safety messages with pupils routinely, wherever suitable opportunities arise
▪ Reminding pupils, colleagues and parents/carers about their responsibilities, which have been agreed through the User Agreement that all pupils and parents/carers have signed
▪ Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements
▪ Teaching pupils as a planned element of personal, social, health, economic and citizenship education about online safety, cyber-bulling, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

MANAGING AND SAFEGUARDING COMPUTER SYSTEMS

It is our leadership team's role to ensure that the security of the school's systems and its users are reviewed regularly. To support the maintenance of the school's systems:
▪ Virus protection is installed and current on all laptops used for school activity
▪ Access by wireless devices is proactively managed (pupils cannot access the school's wireless network from their personal devices)
▪ Portable media may not be used without specific permission
▪ Mobile Device Management is deployed across devices on and off site which allows leader to monitor and secure devices remotely via an internet connection
▪ Unapproved software is not allowed on any school machines
▪ Any administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, e.g. head teacher and the designated safeguarding lead.
▪ No-one except the IT consultants, Head Teacher or designated safeguarding lead is allowed to download and install software onto the network
▪ New users can only be created and approved by a member of the leadership team
▪Any laptops or school technology taken off the school site must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the staff member

INTERNET ACCESS

The school maintains a simple internet connection that requires a password to access. This password is not shared with pupils, but visitors are able to use it to connect to the internet if required. Through use of the 'Google Classroom' staff are able to give pupils access to the internet through a mobile hotspot. This can be withdrawn via the handset in possession of the staff member and leaders can also shut down or restricted devices remotely if needed. Pupil profiles are set to maximum restriction and leaders are able to monitor, track and restrict internet and computer access remotely. Leaders can also restrict or approve websites as required.

EMAIL

Email is regarded as an essential means of communication and all employees are provided with an e-mail account. Communication by email from teaching staff and administration staff to parents/carers and to external organisations should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained.

The same procedures are expected of all other employees who send emails to external organisations and colleagues. Use of the school's e-mail system is monitored and checked and staff should not use personal email accounts during school hours or for professional purposes. Staff are not permitted to use school email accounts to communicate with pupils directly at any time. See our data protection policy for further information on use of email and storing documents on Google Drive.

PUBLISHING MATERIAL ONLINE

SIS maintains editorial responsibility for website content to ensure that the content is accurate and the quality of presentation is maintained. The schools maintain the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The identities of pupils are protected at all times.

Photographs of identifiable individual pupils are not published on the website unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs never have names attached

Pupils publishing online (blogs and websites)

In some instances, it may be appropriate for pupils to use websites or blogs to complete, or celebrate, their work. As always, the identities of pupils must be protected at all times. Photographs of identifiable individual pupils are not published unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs must never have full names attached (first name or initials only) and no personal information that could be used to identify them should be disclosed.
Parents/carers must have given specific permission via the user agreement forms to allow pupils to create websites or blogs.

Other online communication platforms

Staff and pupils are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing

inside and outside of school hours. Material published by pupils and staff in a social context which is considered to bring the school's reputation into disrepute or considered harmful to, or harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per behaviour, equality, antibullying and/or staff conduct policies/procedures.

USING IMAGES, VIDEO AND SOUND

SIS recognises that many aspects of the curriculum can be enhanced by the use of multimedia and that there are now a wide and growing range of devices on which this can be accomplished.

Pupils are encouraged and taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

All parents/carers are asked to sign an agreement about taking and publishing photographs and video of their pupils when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed. For their own protection staff or other visitors to our premises are discouraged from using a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils or visitors.

MOBILE PHONES

Pupils are discouraged from bringing mobile phones into school but if they do they typically hand them to the school offices for safe keeping until the end of the school day. Some pupils may keep their mobile School staff are not to use mobile phones during the school day, with the exception of calling the school or the emergency services if an emergency situation arises whilst off-site (eg. school trips).

Staff are not encouraged or expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber-bullying', will be considered a disciplinary matter for pupils and staff alike. The same is the case for other inappropriate use of mobile technology, such as 'sexting'. Pupils are taught about misuse of technology as a matter of course through the school's personal, social, health, economic and citizenship education programme. See our 'what we do' policy for curriculum information.

NEW TECHNOLOGY

SIS will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view. We will regularly

review this policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Employees, visitors or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

DATA

The school recognises their obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically.

We ensure:

▪ Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties
▪ Staff are aware of their obligation to keep sensitive data secure when working on computers outside of school
▪ When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
▪ There is full back up and recovery procedures in place for school data (all child and staff data is kept securely in the 'cloud' online).
▪ Where sensitive, staff or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies
▪ Please also refer to our Data Protection policy.

ONLINE SAFETY INCIDENTS

All incidents, including online safety incidents, are recorded on our incident sheets. Any incidents where pupils do not follow the User Agreement will be dealt with following the school's 'how we do it' (behaviour policy) and procedures. In situations where a member of staff is made aware of a serious online safety incident, concerning pupils, visitors or staff, they will inform a senior leader who will respond in the most appropriate manner. Instances of cyber-bullying will be taken very seriously and will be dealt with using the school's preventing bullying procedures and the organisation's disciplinary procedures.

The organisation recognises that staff as well as pupils may be victims and will take appropriate action in either situation. If an action breaches school policy, appropriate sanctions will be applied. The schools will decide if parents/carers need to be informed if there is a risk that child data has been lost. SIS reserves the right to monitor their premises equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

GOVERNANCE

The Education (Independent School Standards) Regulations apply a duty to proprietors of independent schools to ensure that arrangements are made to safeguard and promote the welfare of children. The body of governance at SIS consists of a governing body. The governing bodies ensure that they comply with

their duties under legislation and fulfil their duty to remedy any weaknesses that are identified.
In relation to online safety, duties and responsibilities include:

▪ The proprietor and governors will ensure that appropriate filters and monitoring systems are in place, across all of the sites to ensure that pupils are safeguarded from potentially harmful and inappropriate material
▪ The proprietor and governing body will ensure that children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.

PUPIL COMPUTER & INTERNET USER AGREEMENT THIS MUST BE SIGNED BY BOTH PUPIL AND PARENT/CARER BEFORE INTERNET ACCESS IS ALLOWED

Use of ICT considers the use of the school's technology and internet. As part of a society that where technology is used regularly, pupils must have the opportunity to learn appropriate and positive ways of using technology. At SIS, pupils are expected to be responsible for their own behaviour on computers and the internet, just as they are anywhere else in school.

In order for us to allow internet use, pupil and parents must read and agree to the Use of ICT Agreement.

Use of ICT Agreement:

▪ I will only access the system through the proper log-in and will keep my password secret from others
▪ I will not access other people's files
▪ I will only use the computers for school work and homework
▪ I will not bring CDs or other storage devices from outside school unless I have been given permission by a teacher
▪ I will not use rude language in my work
▪ I will ask permission from a member of staff before using the internet
▪ I will not download any files from the internet
▪ I will not try to access social media sites or instant messaging services
▪ I will not email people unless teachers approve it
▪ I will never give out my personal details online
▪ If I see anything rude, or anything that worries or upsets me, I will tell a teacher immediately
▪ I understand the school may check my computer files and internet usage
▪ I will only use approved websites and all communications will be supervised and appropriate
▪ I know that if I break these rules, I may lose access to the computers and internet in school

If parents have any concerns about their child and their use of ICT in or out of school, or would like to request support in ensuring their home is secure and has the appropriate parental controls in place, please contact a member of staff and we will make every effort to support you.

Name Date Sign

Noreen Rahman
Head Teacher

Date: 15 July 2020

Review Date: 15 July 2021

Seva Care Group Ltd
Company Registration Number: 06496694.
Registered office address: 14 College Road, Harrow. HA1 1BE.
Telephone: 020 8422 2999.