SUNNYDOWN SCHOOL

Portley House, 152 Whyteleafe Road, Caterham, Surrey, CR3 5ED
t. 01883 342281 / 346502 **f.** 01883 341342
e. office@sunnydown.surrey.sch.uk
www.sunnydown.surrey.sch.uk
Headteacher Mr Paul Jensen B.Ed Grad Dip (SEBD) NPQH

Digital Literacy (Online and E-safety) Policy

Review Period: Annual **Status: Non Statutory** **Next review Date: Autumn 23**

Developing and Ensuring Digital Literacy

E-Safety is part of the ***S***chool's commitment to Safeguarding and Child Protection.

This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling, General Data Protection Regulation ***(GDPR)***, Acceptable Use Policy ***(AUP)*** and the use of images.

The Sunnydown Online and E-Safety Policy has been written by the ***S***chool Digital Literacy Committee, building on best practice and government guidance. It has been agreed by senior management and approved by governors.

Our Online and E-Safety Policy

The online and E-Safety policy and its implementation will be reviewed 3 yearly.

The Online and E-Safety Policy covers the use of the increasing range of technology which can access the School network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and handheld games consoles used on the School site.

The Online and E-Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The ***S***chool will provide managed internet access through Eduthing, Senso and LanSchool to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to make them aware of differences between ***S***chool IT systems and the more open systems outside school.

Access to ***S***chool networks will be controlled by personal passwords which should be at least 8 characters long including at least one number. These should be changed every term and permissions to ensure the appropriate users have access. Users will be managed by Eduthing and training for students and staff will be offered to ensure safety of information.

The system is in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform the Online and E-Safety Policy. Any breaches or suspected

breaches are brought to the attention of the Designated Safeguarding Lead (DSL) and will be discussed at the next DSL meeting.

The security of School IT systems will be reviewed regularly by the Managed Service provided by Eduthing.

The effectiveness of filtering and security will be monitored by the DSL team.

Staff responsible for managing the filtering systems or monitoring IT are DSLs or DDSLs and follow the ***S***chool procedure for reporting online safety issues (Appendix Four (4) E-Safety Concerns taken from the Safeguarding and Child Protection Policy 2015 is attached to this policy for reference).

The *S*chool will ensure that access to the internet via *S*chool equipment for anyone not employed by the *S*chool is filtered and monitored.

Internet Use

The *S*chool will provide an appropriate online safety curriculum through PHSE that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. The effectiveness of this will be monitored by the E-Safety *C*ommittee. Special sessions are arranged when required.

The preference is for communication between staff and pupils or families should take place using the ***S***chool systems.

Online and E-safety lessons

Pupils will be advised during their online safety lessons in the curriculum not to give out personal details or information which may identify them or their location. **This policy now includes "sexting", which is when someone shares sexual, naked or semi-naked images or videos of themselves or others, or sends sexually explicit messages (as advised on pages 5 & 6 the UK Council for Child Internet Safety sexting in school document). Any breach will be picked up by the DSL Team and possible outside agencies. For additional information, see section 15 – online safety and 21 – Youth produced sexual imagery (sexting) of the Sunnydown School Child Protection and Safeguarding Policy.**

E-mail

- Communication between staff and pupils will only take place via the approved e-mail accounts (Gmail & Outlook) on the ***S***chool IT systems.
- Initials will be used to reduce the identification of individuals.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Personal device***s*** should not be used to download confidential attachments and will need to be password protected.
- Pupils needing to use email to contact external bodies as part of their education must seek permission from staff. KS3 students will be restricted to emailing staff and students within the School.

Published content on the School website and social media

- The contact details will be the School address, email and telephone number. Staff or pupils' personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- If referred to, students will be identified by first name only to reduce the potential identification of individuals.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the School website or any ***S*chool-run** social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/your-council/about-our-website/photographs-of-children-and-young-people

Use of social media including the school learning platform

- The School will control access to social networking sites, and consider how to educate pupils in their safe use.
- Use of video services such as Skype, Google Hangouts and Facetime will be managed and monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in-school and out-of-school takes into account the feelings of others and is appropriate for their situation as a member of the School community.

Use of personal devices

- Please refer to guidance contained with respective AUP. ***(Acceptable Use Policy)***

Protecting personal data

- The School has a separate Data Protection Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to School systems.

Policy Decisions Authorising access

- All staff (including teaching assistants, support staff, office staff, student teachers, work experience trainees, ICT technicians and governors) must read and sign the Staff AUP (Acceptable Use Policy) before accessing the school IT systems
- Pupils must apply for internet access individually by agreeing to comply with the student AUP when they sign this document. Parents will also be asked to sign and return this document. Copies of these signed agreements are kept on student files.
- Visitors to the school must read and sign the Visitor AUP ***(Acceptable Use Policy)*** before being given access to the internet or use School equipment.

Assessing risks

- The ***S*chool** will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer. Neither the School nor Surrey County council (SCC) can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with according to the School Behaviour Policy.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding and Child Protection Policy

Communication of the Policy

To pupils

- **All existing and new Pupils will need to know what an AUP Acceptable Use Policy is and sign one before using any systems.** Pupils need to agree to comply with the pupil AUP in order to gain access to the ***S***chool IT systems and to the internet on an annual basis by signing an AUP

To staff

- **All and new members of staff will need to know what an AUP Acceptable Use Policy is and sign one before using any systems.**
- All staff will be shown where to access the Online Safety Policy and its importance explained
- All staff will receive online safety training on an annual basis.
- Failure to deliberately uphold the conditions set out in this Policy and the AUP will be considered through the Disciplinary Procedure This policy alongside the Staff AUP includes the use of personal mobile devices while on site.

To parents

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters and on the School website.
- Parents will be offered online safety training annually through the newsletter.
- Parent signatures on the Pupil AUP will be annually updated.
- This Policy alongside the Staff AUP includes the use of personal mobile devices while on site.