

# THE STOKE POGES SCHOOL

## Online Safety Policy

<b>Governors Committee Responsible for the Policy</b>	Teaching and Learning Committee
<b>Date Approved</b>	September 2019
<b>Recommended Review Period</b>	Annual
<b>Date for Review</b>	September 2020
<b>Person Responsible for the Policy</b>	Computing Lead

The implementation of this Online Safety policy will be monitored by the:	Rani Makkar (Online Safety Coordinator)
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Rani Makkar, Liz Astley, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents to be kept in Head's office or on CPoms
- Monitoring logs of internet activity (including sites visited) and filtering via Updata (ISP provider from Buckinghamshire County Council)

### Scope of the Policy

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

### Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

#### Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. Ed Bramley-Harker has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety parent meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering provided by the IT support
- reporting back to relevant Governor meetings

#### Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Headteacher and the Online Safety Coordinator should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

The Headteacher is responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

The Headteacher and Governors will receive regular monitoring reports from the Online Safety Coordinator.

#### Online Safety Coordinator

- leads the Online Safety policy
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering
- attends relevant meeting of Governors
- reports regularly to Senior Leadership Team

#### Network Manager and Technical staff

The Network Manager and Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online Safety Officer Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

#### Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher and Online Safety Officer Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### Designated Safeguarding Lead

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

### Students:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- 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

### Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

### **Policy Statements**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should 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.

Pupils should 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 in lessons where internet use is pre-planned. It is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

	School Devices		Personal Devices	
	School owned for single user (laptops, desktops, ipads)	School owned for multiple users	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	
Internet only	Yes	Yes	Yes	
No network access				Yes

**Review**

This policy will be reviewed annually and the Headteacher and Online Coordinator will monitor classroom practice for evidence of implementation.

<b>Headteacher</b>		<b>Date</b>	
<b>Chair of Teaching and Learning Committee</b>		<b>Date</b>	