Signature and date
[FGB/committee chair]

Slimbridge Primary School Policy
Approved: September 2020
To review: Annually

Slimbridge Primary School
Online safety Policy

Safeguarding is a serious matter; at Slimbridge Primary School we use technology and the Internet extensively across all areas of the curriculum. This policy aims to safeguard children by promoting appropriate and acceptable use of IT and outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work-related IT systems
It will be reviewed on an annual basis or in response to a safety incident, whichever is sooner.

This policy is available for anybody to read on our School website; upon review all members of staff will sign to confirm they have read and understood both the Online Safety Policy and the Staff Acceptable Use Agreement. The Student's Acceptable Use Agreement will be shared and discussed with the children at the beginning of each term and will be displayed in the classroom. A copy of the Acceptable Use Agreement will be sent home at the start of each year. 'Be SMART on the internet' will be displayed in each classroom.

Roles and Responsibilities

At Slimbridge Primary School, all staff, together with the governing body, share responsibility for the safeguarding of our children. Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. All staff, Governors and visitors at Slimbridge Primary School must be aware of the following responsibilities in order to ensure safe and responsible use of technology.

Professional and personal safety

* All staff, Governors and visitors understand that they are responsible for all activity carried out under their username. Usernames or passwords must not be disclosed to anyone else.

* All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices.

* If an online safety incident should occur, staff, Governors and visitors will report it to the Senior or Deputy Designated Professional for Child Protection as soon as possible, in line with the school's Safeguarding Policy

Professionalism in communications and actions when using school ICT systems

* All staff, Governors and visitors will only use the school's email / internet / intranet etc. and any related technologies for uses permitted by the Head or Governing Body. If anyone is unsure about an intended use, they should speak to the Head beforehand.

* All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body, in line with the GDPR procedures.

* Personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business. Each class has an ipad specifically for this purpose. These should NEVER be used for personal use.

* Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. Filming and photography by parents and the wider community at school events, such as sports days and school productions, are not allowed. When possible, parents/carers will be given the opportunity to take individual photographs, for example in their play costumes.

Provision of safe and secure access to technologies and ensure the smooth running of the school:

* Staff, Governors and visitors will not install any hardware or software on any school owned device without the Head's permission.

* All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

* All staff, Governors and visitors will only use the approved email system for school business.

* All staff, Governors and visitors will make every effort to comply with copyright and intellectual property rights.

* All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head in line with our school's Safeguarding Policy

Governing Body

The governing body is accountable for ensuring that our school has an effective Online Safety Policy and has overall responsibility for the governance of online safety and acceptable use of technology throughout the school. The governing body has a responsibility to review this policy annually and ensure the following:

- it is up-to-date and covers all technology use within the school.
- it takes into consideration the changing use of technologies and new threats to online safety ensuring that the school is up-to-date with emerging risks and threats through the use of technology.
- the school's incident log is regularly checked for any online safety incidents and ensure that they have been dealt with appropriately and effectively in line with this policy.
- regular updates are received from the Headteacher or Computing Lead Teacher, in regards to training, any identified risks or any incidents.
- the Acceptable use agreements are implemented, monitored and reviewed regularly, and all updates are shared with relevant individuals at the earliest opportunity
- allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our school. The Headteacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team, the governing body, and parents.
- Retain responsibility for the online safety incident log and ensure that all incidents are dealt with promptly and appropriately.
- *All staff know when and what to report* should an online safeguarding issue arise.
- Engage with parents and the school community on online safety matters at school and/or at home.

- Ensure any technical online safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.

All Staff

All staff, especially those who are responsible for the teaching of Computing, are responsible for ensuring that all children in their care are safe whilst using the internet. All teachers will be provided with a copy of the Online safety policy. The use of personal technologies will be subject to the authorisation of the DSL, and such use will be open to scrutiny, monitoring and review.

Al staff will:

- Ensure that all details within this policy have been read and understood and that the Acceptable use agreement has been signed
- Ensure that any online safety incident is reported to the Headteacher and an incident report is made
- Familiarise themselves with the latest available resources for school and home use
- Keep up to date with the latest risks to children whilst using technology

- Ensure that children know how to recognise and report a concern

- social media posts relating to the school Twitter account or Class 5 blog will promote the school in a positive light, will not show children's faces nor have the names of any children in

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Operating system updates are regularly monitored and devices updated as appropriate
- Any online safety technical solutions such as Internet filtering are operating correctly
- Filtering levels are applied appropriately
- Passwords are applied correctly to all users regardless of age
- Passwords for staff will be a minimum of 8 characters

All Students

The boundaries of use of ICT equipment and the Internet in this school are given in the student Acceptable Use Agreement. Any misuse of ICT equipment or the Internet will be dealt with in accordance with the behaviour policy.
All pupils will be expected to abide by the Acceptable Use agreement
Online Safety is embedded into our curriculum through the teaching of Computing, PSHE and SRE. Children will be given the appropriate advice and guidance by staff on how to use the Internet safely and appropriately. Similarly, all children will be fully aware of how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents and carers play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters and website updates, the school will keep parents up to date with new and emerging online safety risks, and will involve them in strategies to ensure that children are empowered to deal with them appropriately and maturely.

Parents and carers must also understand that the school needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will read through the student Acceptable Use Agreement with their child so they are both fully aware of the importance of staying safe online and respecting school property.

Technology

Slimbridge Primary School uses a range of devices including PCs, laptops, tablets, visualisers and digital cameras on a daily basis as teaching and learning aids. In order to safeguard our students we employ the following:

Internet Filtering – Our Internet is filtered through the SWgFL (South West Grid for Learning) which prevents unauthorised access to illegal and inappropriate websites. The governing body, Headteacher and equally, the teaching staff as a whole, are responsible for ensuring that the filtering is appropriate.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998 and with reference to GDPR procedures) and are kept on school property are encrypted. No data is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain

whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff are unable to access any computer, laptop or tablet without a username or password. Students can access laptops and classroom computers with year group logins and passwords.

Anti-Virus – All capable devices have anti-virus software. This software is regularly updated for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff and students will be supervised when accessing the internet in school. Parents will be notified about the ways in which Internet use may be monitored.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the school email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted. Children do not have school email accounts and are not permitted to use personal emails whilst at school.

Photos and videos – The use of digital media, such as photos and videos, including camera phones, are covered in the schools' 'Photographic Policy', and is re-iterated here for clarity. Photographs and videos of children are regularly taken throughout the school year. This is for a number of purposes, namely: to provide evidence of learning and assessment, to record achievements and celebrate success. We also use photographs and videos as a way of preserving memories for the future. Images and video footage are taken on school i-pads or school cameras. We also have dedicated memory cards for such purposes. Images and video footage are stored on the school computer network.

Parents are asked for permission before photography is allowed within school and during school events. A register must be signed and dated stating that any images they take will not be used inappropriately.

The use of camera phones on the school premises can potentially cause risks directly and indirectly to children. Due to this, we have strict rules for the use of camera phones and similar technology whilst at school. Teachers are not permitted to use such technology during the school day or on school excursions; parents are asked to read the safety information prior to signing in and by doing so agree not to use their phones whilst in the school. Further guidelines about the use of camera phones can be found in our Acceptable Use and Photographic Policy.

Social Media – The use of Social Media (i.e. Facebook, Instagram, Snapchat etc.) is not permitted at school by adults *or* children. However, children in KS2 may be encouraged to contribute to online class blogs, which are safe, regularly monitored and fully moderated. The school has a Twitter site and this is managed by the IT co-ordinator.

Incidents - Any online safety incident is to be brought to the immediate attention of the Headteacher, a member of the SLT or the Governor responsible for Safeguarding. Incidents will be recorded in the Safeguarding log and brought to the attention of the Governing Body.

Training - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Slimbridge Primary School will have an annual programme of training which is suitable to the audience. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher.

Online Safety and the Curriculum – Safeguarding children online is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. Each class has an Online Safety display and the school has adopted Childnet's 'Be Smart on the Internet' rules to help children become more aware of their personal responsibilities.

Each Key Stage follows an online safety curriculum which is tailored to their specific age (see Computing Policy which outlines the strategies and resources used to develop children's awareness of staying safe whilst online). Online teaching programmes and resources such as: www.thinkuknow.co.uk and www.bbcbitesize.co.uk are regularly used in both KS1 and KS2 as a teaching aid. The 'Hector's World Safety Button' is a child-activated safeguarding tool which children use if something on-screen upsets or worries them. Children in upper KS2 receive an annual visit from the local police to discuss online safety issues with children; their parents are also invited to attend.

This policy should be read in conjunction with the following:

Computing Policy
Acceptable Use of Internet Policy
Sex and Relationship Policy (SRE)
Safeguarding Policy
Photographic Policy
Anti-bullying Policy