Signature and date
[FGB/committee chair]

Slimbridge Primary School Policy
Approved: Sept 2016
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. Online safeguarding is an area that is constantly evolving and as such this policy 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 as read and understood both the Oneline Safety Policy and the Staff Acceptable Use Policy. A copy of the Student's Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Roles and Responsibilities

At Slimbridge Primary School, all staff, together with the governing body, share responsibility for the safeguarding of our children whilst using the internet.

Governing Body

The governing body is accountable for ensuring that our school has an effective Online Safety Policy and procedures in place and has overall responsibility for the governance of e-safety throughout the school. Their key responsibilities are as follows:

- Reviewing this policy regularly to ensure that it is up to date and covers all technology use within the school
- Reviewing the policy should any incidents occur
- To ensure any online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- To keep up to date with emerging risks and threats through the use of technology
- To regularly check the incident log for any online safety incidents
- To receive regular updates from the Headteacher or Computing lead teacher, in regards to training, any identified risks or any incidents.

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 and governing body, parents.
- Retain responsibility for the online safety incident log and ensure that all incidents are dealt with promptly and appropriately.
- All staff know 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. Therefore, all staff will:

- Ensure that all details within this policy are understood
- 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

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 Policy. Any misuse of ICT equipment or the Internet will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; children will be given the appropriate advice and guidance by staff. Similarly all children will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents 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 parents evenings, school newsletters and updates, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or Internet.

Technology

Slimbridge Primary School uses a range of devices including PCs, laptops, tablets 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 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.

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 (upon signing this Online Safety policy and the staff Acceptable Use Policy) and students (upon signing and returning their acceptance of the Acceptable Use Policy). 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 also discouraged from using them. 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, Twitter, Instagram) is not permitted at school by adults or children. However, children in KS2 are regularly encouraged to contribute to online class blogs, which are safe, regularly monitored and fully moderated.

Incidents - Any online safety incident is to be brought to the immediate attention of the Headteacher or in his/her absence a member of the SLT or governing body committee.

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 for further CPD.

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 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.