E SAFETY POLICY

LYDBROOK PRIMARY SCHOOL
(Including Robins Nursery)

(Version 1)

Revision Record of Published Versions			
Author	Revision Date	Version	Status
Lydbrook Primary	February 2018	1.0	Reviewed and updated by staff
	02/05/2018	1.0	Approved by FGB

1.0 Introduction

Aims

Access to life-long learning and employment increasingly requires the use of a range of information technologies and pupils need to develop skills for their use. The internet, as an open, public communications channel is just one aspect of this. This Policy relates to the School's Internet environment and is part of a suite of e-safety documents and strategies developed to ensure pupils are provided with as safe and secure Internet environment as is possible, and are educated to be aware of, and respond responsibly, to any risks.

The Policy identifies the measures in place in our school:-

- To protect children from undesirable content on the Internet
- To protect them from undesirable contacts over the Internet,
- To prevent unacceptable use of the Internet by children or adults
- To address issues of copyright for materials published on the Internet.

This Policy should be read in conjunction with the Child Protection and Safeguarding Policy.

Roles and Responsibilities

E-safety is a whole-school responsibility dependent on all stakeholders eg. staff, governors, advisers, parents and, where appropriate, pupils themselves taking responsibility for the use of the internet and other forms of communication. Of major importance in creating a safe e-learning environment is the internet safety education which occurs in the classroom itself, initiated by the teacher or teaching assistant.

Online Safety Group

E Safety is supported throughout the school by an E-Safety group with representatives from teachers, support staff, governors, parents, the Designated Safeguarding Lead, Senior Leadership team. Membership of the E-Safety Group is displayed in the staff room. The group is also responsible for issues regarding online safety and the monitoring of the E-Safety policy including the impact of initiatives.

Teaching and Support Staff
Are responsible for ensuring that:
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)

Designated person for Safeguarding (DSL)
Should be trained in e-safety issues and be aware of the potential for serious child protection 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
- cyber-bullying

E-learning technologies
Internet access is supplied by Gloucestershire County Council and the South West Grid for Learning (SWGfL). This provides an effective and safe e-learning environment including Internet access and e-mail service. To safeguard against risks and unacceptable materials and activities, these services include filtering and content control, firewall and virus protection, and monitoring systems All new Internet technologies will only be made accessible to the school e-community when they have been assessed for their nature and content, educational benefit, safety and security.

Permission to use the Internet
The internet can provide pupils and all stakeholders with opportunities to experience and use a wide range of activities, resources and information to support and enhance the learning and teaching across the whole school curriculum. All pupils will be expected to access the Internet unless parents have indicated otherwise at the time their child is admitted to school.

Pupils are responsible for using the school ICT systems in accordance with the **Pupil Acceptable Use Policy**, which they will be expected to sign before being given access to school systems.

Parents will be asked to discuss with their children the Pupil Acceptable Use Policy and get their child to sign the Agreement. Without this being signed, pupils will not be allowed to access the internet.

In addition, parents will be required to sign an Acceptable Use Policy which supports their child's understanding and use of the internet safely at home and all other times.

Access and using the Internet
In lessons the majority of access to the Internet will be by the teacher, by adult demonstration or through carefully supervised access to specific approved on-line materials. Pupils will be taught how to use the internet safely and responsibly as an integral part of e-learning across the curriculum and supported by the school's e-safety scheme of work. In the spirt of Every Child Matters pupils will be taught how to be safe online at home as well as at school.

The school's Internet home page will default to a recognised children's search engine as its Home page such as Google.

E-Safety – Content

Unintentional exposure of children to Inappropriate Content

It is the School's Policy that every reasonable step should be taken to prevent exposure of children to undesirable materials on the Internet. It is recognised that this can happen not only through deliberate searching for such materials, but also unintentionally when a justifiable Internet search yields unexpected results.

To protect children from such occurrences, the following in-school protection has been adopted:-

- Adult supervision of pupils' Internet activity, with no accessing or searching of the internet allowed without a suitable adult present in the room.
- The "caching" of Internet sites whenever possible in advance by staff to verify the site and its contents.
- Children will be taught to become critical and discriminating users of materials they find online, through questioning the source and reliability of any content they access and by being aware of ways to minimise risks.
- If any users discover undesirable sites, the URL (address) and content must be reported to the School Business Manager who will inform the Internet Service Provider as soon as possible.
- The use of the accredited County Council Broadband service which provides protection by maintaining a list of approved sites.
- Filtering, such as blocking strategies, allowed lists, dynamic filtering, rating systems, flagging systems and monitoring.
- The imposition of a "banned list" of undesirable sites
- The filtering of sites by language content with prohibition of sites with unacceptable vocabulary.
- "live" anti-virus protection.

Intentional access of undesirable content by children

Deliberate access to undesirable materials by adults is unacceptable, and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted.

Children should never intentionally seek offensive material on the Internet. In such instances these steps will be followed. Any such incident will be treated as a disciplinary matter, and the parents of a child or children will be informed. In the event of children being exposed to undesirable materials, the following steps will be taken:-

- Pupils will notify a teacher or teaching assistant immediately
- Initially the e-safety co-ordinator will be notified by the teacher, and then the Designated Lead for Child Protection.
- The incident will be recorded in a central log, located in the school office, by which the school may reliably report the frequency and nature of incidents to any appropriate party.
- The County approved forensic monitoring software will be used to investigate as appropriate
- Parents will be notified at the discretion of the Headteacher according to the degree of seriousness of the incident.

- The Headteacher will regularly notify Governors of any incidents involving inappropriate or unacceptable use of school internet/ICT facilities as part of the Headteacher's report.

Risks associated with Contact
The Internet as a means to contact people and organisations is an extremely valuable tool, encouraging the development of communication skills and transforming the learning process by opening up extra possibilities. However, just as in the real world, children may get involved in inappropriate, antisocial or illegal behaviour while using new technologies eg. cyber bullying, identify theft, and arranging to meet people they have met online.

Whilst children will, at times, use emails as part of their learning across the curriculum, the school does not use chat rooms or instant messaging. Children will however be made aware of the risks involved in all of these and ways of avoiding them, as part of their e-safety and digital literacy skills development.

Receiving and sending of emails by children
It is recognised that e-mail messages received by children can contain language or content that is unacceptable and that some people may try to use e-mail to identify and contact children for unacceptable reasons. If any staff believe that a child has been targeted with an e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the child's parents informed. Advice will also be taken regarding possible further stops, including investigation using forensic monitoring software.

To avoid these problems the school has adopted the following practice:
- The use of the accredited County email service which includes filtering all incoming and outgoing messages for inappropriate content and spam.
- Pupils read e-mail messages when a member of staff is present, or the messages have been previewed by the teacher.
- Children are taught not to open or respond to emails from a previously unknown source, but to tell the member of staff present in the room so that appropriate action can be taken.
- Steps are taken to verify the identity of any school or child seeking to establish regular e-mail with this school.
- Pupils save their emails/messages to draft for the teacher or teaching assistant to approve before being sent (as they would with a conventional letter)
- To avoid children revealing their identity within email messages, only the child's forename is revealed: when appropriate "internet aliases" are used for each child: the child's personal address is never revealed and information is never given that might reveal the child's whereabouts.

Other use of the Internet and email facilities
The school internet/email facilities should only be used for educational purposes during teaching and learning time. Staff are advised not to, but if they do choose to use school internet facilities for personal purposes, such as online banking or purchasing of items for personal use, this will be at their own risk.
Inappropriate use will be subject to similar procedures as those listed above.
Staff should be mindful of unsolicited emails from people they do not know and use the spam reporting facility as appropriate.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site, VLE*
- *Parents evenings*
- *Reference to the SWGfL Safe website (nb the SWGfL "Golden Rules" for parents)*

Education - Extended Schools
The school will offer family learning courses in ICT and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Publishing of Content on the Internet

It is recognised that staff and children may at some time produce and publish materials on an Internet Website associated with the school or the County. The school has its own website hosted through its recognised reputable ISP. Materials produced as part of children's learning may be published on it unless parents have indicated otherwise at the time their child is admitted to school. No materials will be published on the Internet which contain any unacceptable images, language or content. Infringement of this rule will be taken as a serious disciplinary issue.

Use of the school's Internet facility by visitors and guests

Members of school staff are expected to take responsibility for the actions of any adult guests or visitors who they allow or encourage to use the school Internet facilities. The essential "dos and don'ts" are explained to new visitors and guests prior to their use of the Internet.

Unacceptable use will lead to the immediate withdrawal of permission to use the School Internet facilities.

Technical – infrastructure / equipment, filtering and monitoring
The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school ICT systems.
- All users (including pupils at KS1 and KS2 will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head Teacher or other nominated senior leader and kept in a secure place (eg school safe)
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL
- Requests from staff for sites to be removed from the filtered list will be considered by the School Business Manager and the E-Safety Co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. Remote management tools are used by staff to control workstations and view users activity.
- An appropriate system is in place (incident log book) for users to report any actual / potential e-safety incident to the School Business Manager).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices (Staff Acceptable User Policy and Data Protection Policy).
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third party materials contained within them.

Related documents

Safeguarding and Child Protection Policy

Acceptable Use Policy – Staff

Acceptable Use Policy – Foundation and KS1 pupils

Acceptable Use Policy – KS2 pupils

Acceptable Use Policy – Parent/Carer

Data Protection Policy

This e-safety policy was approved by the *Governing Body on*	2nd May 2018
The implementation of this e-safety policy will be monitored by the:	*E-Safety Group*
Monitoring will take place at regular intervals:	*3 times per year*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*February 2019*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Police Gloucestershire Childrens' Safeguarding Board SWGfL
Signed	T. Roberts, Chair of Governors