PARSLOES PRIMARY SCHOOL

E-Safety Policy
2017/2018

Submitted for Approval by Governing Body: March 2018
Review Date: March 2019

Michael Corcoran
(Executive Headteacher)

Richard Hunter
(Chair of Governors)

Ross Johnson
(ICT Leader)

Spurling Road
Dagenham
Essex
RM95RH
02082704925

Updated March 2018

PARSLOES PRIMARY SCHOOL

School Policy Statement
For
E-SAFETY

RATIONALE

Our e-Safety Policy builds upon government guidance, to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The Internet is now considered to be an essential part of modern life. In addition, the school has a duty to provide pupils with quality Internet access as part of their learning. This e-safety policy considers the use of both the fixed and mobile internet, PCs, laptops, webcams, digital video equipment, mobile phones, camera phones, portable media players and tablet computers. It will be revised to incorporate new and emerging technologies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

PURPOSES

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.

The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies

WRITING AND REVIEWING THE E-SAFETY POLICY

The e-safety policy relates to other policies including those for ICT, anti-bullying, child protection and data protection.

The e-safety co-ordinator is Ross Johnson

The Designated Child Protection Lead is Mrs Karen Deville (Deputy Head teacher), our Deputy Designated Lead is Mrs Lauren Pearce (Head of School)

KEY LINKS FOR E-SAFETY

Please visit the following links which support our E-Safety Policy:

www.thinkuknow.com

safe.met.police.uk

TEACHING AND LEARNING

How we manage the risks:

a) The school Internet access is through the secure, filtered broadband from the London Grid for Learning (LGfL).
b) The school uses CC4 network system, which complies with the National Education Network standards and specifications.

c) A Virus protection system is installed on all computers in school and the school checks that this protection is updating regularly and informs the LA of any issues. Any portable media brought into the school must have permission from the E-Safety Co-ordinator and will be subject to a virus check.
d) The school will work with the LA to ensure systems to protect pupils are reviewed and improved.
e) The headteacher ensures that the e-safety policy is implemented and compliance with the policy monitored. Some material available on the Internet is unsuitable for pupils. Methods to identify, assess and minimise risks will be reviewed regularly. The school will take all reasonable precautions to ensure that pupils access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
f) Where unsuitable content is encountered staff and pupils should follow the school procedures for such events. Report any instance of inappropriate sites that come through the filter system to either the ICT Manager, who can block these and who will inform the Head Teacher, or the Head Teacher directly, so that they can blocked. The Head Teacher and ICT Manager can block these through RM filter manager. Also with CC4 we can as a school block certain website addresses or allow only certain website addresses.
g) Emerging technologies will be examined for educational benefit and any risk considered before use in school is allowed, e.g. Google Classroom

Internet use to enhance learning

1. Pupil access to the Internet will be by adult demonstration or directly supervised access to specific, approved on-line materials. Instruction in responsible and safe use by pupils will precede Internet access.
2. As part of the curriculum, pupils will be made aware of the guidelines for the acceptable use of the Internet and what is not acceptable. These guidelines for acceptable use will be clearly on display in all areas of the school where Internet access is available.
3. With CC4, every time a pupil logs on, our E-Safety rules will need to be agreed to before the pupil can proceed.
4. All pupils will be given clear objectives when using the Internet. Where Internet activities are part of the curriculum they will be planned so that they enrich and extend the learning activities. Staff will guide pupils through on-line activities that will support the learning outcomes planned for the age and maturity of the pupils.
5. All websites used for specific activities will have been approved by the school.
6. Curriculum activities that involve the use of the Internet for gathering information and resources will develop pupil skills in locating and evaluating materials. Pupils will be taught how to validate materials they read before accepting their accuracy. The use of search engines will be restricted to school approved search engines. Other techniques for research will be developed through the use of a limited group of school approved sites. Where materials gathered from the Internet are used by pupils in their own work, they will be taught to acknowledge the source of information used. The school will ensure that the use of Internet materials by staff and pupils complies with copyright law.

E-Mail

1. Curriculum activities that involve the use of e-mail will be through the use of class or group webmail accounts that are controlled by the school.
2. The use of individual pupil personal accounts will not be permitted through the school system. Pupils will have own learning gateway logins, they can only e-mail within our school community as part of curriculum lessons. Ability to e-mail other schools outside the borough and to other schools worldwide, through our international links, must be approved by SLT.
3. Pupils must immediately report to an appropriate member of staff if they receive any offensive e-mail.
4. In e-mail communications, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

5. All e-mail communications sent by members of staff that relate to the school will be through the borough's learning gateway. Staff should not use own personal e-mail addresses for work related e-mails and equally school e-mail addresses should not be used for non-work related e-mails.

PUBLISHED CONTENT AND USE OF IMAGES OF CHILDREN

1. Parents/ guardians will be asked to at the beginning of each year as to whether they give their permission for photographs taken in school can be used in the press or on the school website.
2. Staff or pupil personal contact information is not published. The contact detail for the school on our website is the main school office.
3. Staff only use school devices for photographing learning activities.
4. Staff have clear guidelines, particularly in the Early Years Foundation Stage, relating to no use of personal mobile phones/devices during teaching sessions when children are present.
5. The school website is maintained and kept up to date. The headteacher ensures that the content is accurate and appropriate to the needs of the school community. No personal information about any member of the school community will be published on the website. Any photographs published will not allow individual pupils to be identified.

In addition to this we follow the guidelines below:

- We do not use children's names in photograph captions. If a child is named, avoid using the photograph.
- Only use images of children in suitable clothing to reduce the risk of inappropriate use.
- We State clear expectations of professional photographers or the press who are invited to an event. These make clear the organisation's expectations of them in relation to child protection.
- We do not allow photographers unsupervised access to children.
- We do not approve photography sessions outside the event or at a child's home.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Social Media – Staff

- The school has clear reporting guidance, including responsibilities, procedures and sanctions
- All school staff sign the Acceptable Use Agreement indicating they understand and will follow the guidance contained
- School staff ensure they make no reference in social media to pupils, parents / carers or school staff or the school directly
- School staff should not engage in online discussion on personal matters relating to members of the school community
- School staff should ensure that personal opinions are not attributed to the school or local authority
- School staff should ensure that security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- The school should effectively respond to social media comments made by others according to a defined policy or process

Social Media – Pupils

- The use of online chat rooms, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the pupils.
- Pupils in years 5 & 6 can be allowed to use moderated social networking sites such as Grid Club.
- Pupils will always be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Social networking sites such as Facebook, Instagram or MySpace are not allowed to be accessed through our network or during working hours
- If these sites are used outside of school, staff should not have any past or present pupils as their friends on such sites.
- Staff should not access these sites while at school.

INCIDENT MANAGEMENT

Responding to Incidents

- The school will take all reasonable precautions to ensure online safety
- Complaints of internet misuse will be dealt with by a senior member of staff, with Online Safety Coordinator as first point of contact
- Any complaint about staff misuse must be referred to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the Local Authority's Designated Officer
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- If a member of staff or pupil receives online communication that is considered particularly disturbing or illegal, the Police will be contacted
- If an incident involving sexting comes to the attention of a member of staff, it must be reported to the Designated Safeguarding Lead immediately (see appendix 2 for further advice relating to sexting incidents)
- Complaints related to cyberbullying will be dealt with in accordance with school bullying procedures
- Monitoring of incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents / carers are informed of online safety incidents involving children and young people for whom they are responsible

OTHER TECHNOLOGIES

1. Pupils are not allowed to bring mobile phones into school. In the event of this happening these are kept in the school office until the end of the day. For older pupils who come to school by themselves parents can request that they bring their phone into school but with the understanding that it will be kept in the school safe until the end of the school day. This is to avoid the possibility of the sending of abusive or inappropriate text messages, accessing the internet not through a filtered system.
2. The school has a Skype account and this can only be used as a teaching tool.
3. The school now has undergone the Google classroom technology where children can use the chrome books to access Google apps in order to enhance their learning.

AUTHORISING INTERNET ACCESS

1. All staff must select that they agree to our e-safety agreement before logging on to a computer using any Internet resource in school. Staff will be made aware that Internet traffic can be monitored and traced to the individual user and professional conduct is essential.

2. Parents/carers will sign a consent form giving their permission for their child to use the Internet in school. If parents do not wish their child to continue to use the internet in school this is indicated on the emergency contact form issued at the beginning of each academic year
3. All pupils new to the school are required to complete an Internet permission slip as part of the admission procedure (for those pupils in Key Stage 2)
4. Pupil access may be withdrawn if the acceptable use guidelines are not adhered to.
5. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

COMMUNICATION OF OUR E_SAFETY POLICY

Introducing E_Safety to Pupils

1. E-safety rules will be on display in all rooms where computers are used and will be discussed with pupils regularly
2. Every time pupils use individual .301 logins they will have to agree to our E-Safety Rules.
3. Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
4. A programme of training in e-safety will be developed.
5. As part of the Year 6 curriculum the pupils will participate in an internet proficiency training programme. Details of this programme will be supplied to parents and carers if they wish to use the materials at home.
6. Our Digital Leaders programme will enable children from KS2 to take e-safety training to then deliver to peers and teachers through secure and structured online training

STAFF and the e-safety policy

1. All members of staff including teachers, supply staff, classroom assistants and support staff, will be provided with access to a copy of the school e-safety policy.
2. All staff will be required to agree to our E-Safety policy each time they log on to the network
3. All staff will sign our e-safety agreement before using any internet resource in this school.
4. Staff development in safe and responsible Internet use will be provided as part of the continuing professional development programme.
5. The school will keep an up-to-date record of all staff that have approved Internet access.
6. Staff will always use a child friendly safe search engine when accessing the web with pupils.
7. A list of websites that pupils are not allowed to access is clearly displayed in the ICT suite.

E-safety complaints

Where incidents occur due to non-compliance with the school e-safety policy these will be reported to a delegated senior member of staff. Any issues relating to staff misuse must be referred to the headteacher. Should it become necessary to prohibit the use of internet resources for a pupil then parents or carers will be involved so that a partnership approach can be used to resolve any issues. This could include practical sessions and suggestions for safe Internet use at home.

E-safety for parents

1. Our policy will be in the school prospectus for all new parents and on the school website
2. Annually the school will send out relevant E-Safety information to parents, from resources such as Childnet.
3. Pupils and staff should not have each other as friends on such websites out of school.

Appendix 2

HANDLING A SEXTING INCIDENT

An overview for all teaching and non-teaching staff in schools and colleges

UK Council for Child Internet Safety (UKCCIS)

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as the **production and / or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and / or sexual acts. It is also referred to as 'youth produced sexual imagery'.

Sexting does not include the sharing of sexual photos and videos of under 18-year olds with or by adults. This is a form of child abuse and must be referred to the police.

What to do if an incident involving sexting comes to your attention:

- **Report it to your Designated Safeguarding Lead immediately**
- **Do not** view, download or share the imagery yourself, or ask a child to share or download
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL
- **Do not** delete the imagery or ask the young person to delete it
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- **Do not** share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers
- **Do not** say or do anything to blame or shame any young people involved
- **Do** explain to the child that you need to report it and reassure them that they will receive support and help from the DSL

For further information:

Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016)