



E-SAFETY POLICY

Safeguarding Statement

The Governing Body takes seriously its responsibility under section 11 of the Children Act and duties under *working together* to safeguard and promote the welfare of children; to work together with other agencies to ensure adequate arrangements exist within our setting to identify, and support those children who are suffering harm or are likely to suffer harm.

We recognise that all staff and governors have a full and active part to play in protecting our pupils from harm, and that the child's welfare is our paramount concern. Our school should provide a safe, caring, positive and stimulating environment that promotes the social, physical and moral development of the individual child free from discrimination or bullying where children can learn and develop happily.

This policy applies to all staff, governors and volunteers working in our school. This policy has been written in line with Keeping Children Safe in Education 2016. All staff will sign to confirm they have read and understood this policy.

from Safeguarding and Child Protection Safeguarding Policy updated November 2017

Teaching and Learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

E-mail content and the school web site

- Pupils have internal email addresses and are taught how to use email safely and responsibly. Emails cannot be sent to or received from external email addresses from these internal email addresses.
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility of the school website and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

The school will deny access to social networking sites and students will be advised not to use these at home.

Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the head teacher.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during school time, lockers are provided for safe storage.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- The Headteacher will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school Child Protection Procedures.

Community use of the Internet

All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

Introducing the e-safety policy to pupils

- E-safety Code of Conduct will be discussed with the pupils at the start of each year.
- E-safety Code of Conduct will be on the screens of all pupil laptops so that all users can see it.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- The children receive e-safety lessons and are regularly reminded of online safety.

Staff and the e-safety policy

- All staff will have access to the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic could be monitored.
- Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, and conversations.

If using the internet at home:

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Students should only invite known friends and deny access to others.

Head Teacher's signature.....

Chair of Governors' signature.....

Date: November 2017

Date of next review: November 2018

E-Safety Incident Log

Number:	Reported by: (name of staff member)	Reported to: (eg Head, e-Safety Officer)	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Child Protection Issue?	If yes, complete a Child Protection Record of Concern and inform designated member of staff for child protection (the headteacher)		
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	
Signature (Governor)		Date:	