Whitkirk Primary School

Online Safety Policy

'Be the best that we can be'

This policy applies to members of the Governing Body and volunteers as well as external agencies using the ICT systems at Whitkirk Primary School.

At Whitkirk Primary School, we seek to develop in our children a love of learning that will last a lifetime. Every child in our school is recognised as individual and unique and it is our aim to help them become the best that they can be in a happy and safe atmosphere with the freedom to engage and discover. Our aim is to create a broad and ambitious curriculum which leads to confident, independent learners, who have a passion for learning and are ready for the next step in their education. Our curriculum is knowledge-rich, taking our pupils beyond their own contexts and supports our commitment for all children to have a deep understanding of the world around them. We recognise the Internet as being an integral part of teaching and learning. The Internet can raise educational standards by offering pupils and teachers opportunities to search for information from a wide range of sources and to enhance the child's knowledge of the outside world. As well as providing many benefits and new opportunities, the use of ICT and the Internet, may lead to safety issues for the children. We accept that this must be managed in order to protect the children.

Online safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks. We know that some adults and children will use these technologies to harm students. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

This guidance considers the principles of the Safer Working Practice Guidance (National Safer Recruitment Consortium) as well as guidance from the Department for Education (Safeguarding Children in a Digital World), CEOP (Child Exploitation and Online Protection) and Communication Act 2003 (Section 127 Improper Use of Public Electronic Communications Network). http://www.legislation.gov.uk/ukpga/2003/21/section/127

At Whitkirk, we aim to:

- Educate children to help them to develop a safe, responsible and mature attitude towards Internet use, inside and outside the school environment,
- Regulate Internet access to ensure children are using websites and materials that are appropriate to them,
- All staff to monitor children's access to the Internet both in school,
- Establish home school agreements, involving parents and children and staff about acceptable use of the Internet.

Internet use will support, extend and enhance learning:

- Children will be given clear objectives for Internet use,
- Web content will be subject to age-appropriate filters,
- Internet use will be embedded in the curriculum.

Children will develop an understanding of the uses, importance and limitations of the Online Safety Policy:

- Children will be taught how to effectively use the Internet for research purposes,
- Children will be taught to evaluate information on the Internet,
- Children will be taught how to report inappropriate web content through the use the CEOP button.

- Children will be taught how to report an issue through the “report” button on our school website to report any issues online.

Children will develop a positive attitude to the Internet and develop their ICT capability through both independent and collaborative working:

- Children will use the Internet to enhance their learning experience,
- Children have opportunities to engage in independent and collaborative learning using the Internet and other digital technologies.

Roles and responsibilities:

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regard to training, identified risks and any incidents.

Headteacher:

Reporting to the governing body, the Headteacher has overall responsibility for e-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. children, all staff, governing body and parents.
- All online safety incidents are dealt with promptly and appropriately.

Online Safety Leader:

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst being familiar with the latest research and available resources for school and home use.
- Review this policy regularly.
- Advise the governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log on CPOMS; ensure staff know what to report and ensure the appropriate audit trail.
- Monitor the “Report” button on the school website, should any logs be made.

School staff and volunteers:

- Staff are responsible for their own actions and must act, and be seen to act, in the best interests of children at all times.
- Staff must ensure they understand and adhere to this guidance as well as Whitkirk Primary School’s Acceptable Use Policy.

- Staff are responsible for acting promptly to prevent and safeguard children from potential abuse online and for reporting any concerns in accordance with the Leeds Childrens Services Safeguarding & Child Protection Policy for Schools and Colleges.

ICT Technical Support Staff Technical support staff (RKLT Help Desk) 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
- Windows (or other 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 and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer/Headteacher.
- Passwords are applied correctly to all users regardless of age.

All users:

All users are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online incident is reported to a member of the Safeguarding team (by using the “Report” button on our school website), or via typical communication methods.

All Children:

- The boundaries of use of ICT equipment and services in this school are given in the children’s Acceptable Use Policy; any deviation or misuse of ICT equipment or services 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 and school newsletters, the school will keep parents up to date with new and emerging online safety risks and will involve parents in strategies to ensure that children are empowered. Parents/ carers must also understand the school must have rules in place to ensure that their child can be properly safeguarded. As such parents will sign the children’s Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Prevent:

In order to fulfil the Prevent duty, it is essential that staff can identify children who may be vulnerable to radicalisation, and know what to do when they are identified. Protecting children from the risk of radicalisation is seen as part of schools’ wider safeguarding duties, and is similar in nature to protecting children from other harms (e.g. drugs, gangs, neglect, sexual exploitation), whether these come from within their family or are the product of outside influences. For further information refer to Safeguarding and Child Protection Policy.

January 2021