WISTOW PAROCHIAL C of E PRIMARY SCHOOL

Head Teacher: Carla Cox

E-Safety School Policy

Document Status		
Date of Next Review	**May 2026**	**Responsibility – Full Governing Body**
Date of Policy Creation	**March 2015**	Responsible Governor Name
Date of Review and Ratification at FGB Meeting	**May 2025**	**Allen Blake**
Policy Publication/Communication ☒ On the school website ☒ Shared staff network drive ☒ Updates to staff in staff meetings		*Signed off by the above named Governor during the full governing body meeting held on the date stated as ratified.*

1. INTRODUCTION

This policy has been written based on North Yorkshire E-safety guidance in conjunction with BECTA and CEOP materials. It has been adapted to reflect the school's own decisions on balancing educational benefit with potential risks. The E-Safety Policy will be used in conjunction with policies relating to curriculum, data protection, anti-bullying, safeguarding children, security and home-school agreements.

1.1 This policy has been developed to ensure that all adults and children at Wistow Primary School are working together to safeguard and promote the welfare of pupils.
1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.
1.3 This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect pupils and staff from risks and infringements.
1.4 The Headteacher or, in her absence, the Deputy designated safeguard leader or a member of the School Leadership Team, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 This policy complements and supports other relevant School and Local Authority policies.
1.6 The purpose of internet use in school is to help raise educational standards, promote pupil achievement, support the professional work of staff as well as enhance the school's management information and administration systems.
1.7 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide pupils with quality access as part of their learning experience. The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning, providing they abide by the school rules.
1.8 A risk assessment will be carried out before pupils are allowed to use new technology in schools and settings.

2. **ETHOS**

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.
2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.
2.3 All staff have a responsibility to support e-safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.
2.4 E-safety is a partnership concern and it is not limited to school premises, school equipment or the school day. Parents are partners in e-safety and will be asked along with their children to sign the Home-School Internet User Agreement.
2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the School's Anti-Bullying and Behaviour Policy.
2.6 Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

3. **ROLES AND RESPONSIBILITIES**

3.1 The Headteacher (DSL) will ensure that:

- All staff should be included in e-safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.

- All staff, temporary staff and volunteers are aware of and understand the school's E-Safety Policy and a copy of the policy will be available in every classroom via the staff shared drive.
- They ensure that all staff and volunteers have received a copy of the School's Acceptable Use Agreement.
- A commitment to e-safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- They act as the first point of contact with regards to breaches in safety and security.
- They liaise with the designated person for safeguarding as appropriate.
- They ensure that ICT security is maintained and the school's ICT systems are regularly reviewed and updated. They have a responsibility for "understanding the filtering and monitoring systems and processes in place" as part of their remit.
- They ensure that the virus protection is regularly reviewed and updated.
- They attend appropriate training and update the relevant policies to support and demonstrate this.
- They provide support and training for staff and volunteers on e-safety.
- They will regularly check files on the school's network.

3.2 Governing bodies should ensure that all staff undergo safeguarding and child protection training. It should give them "an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring" The Governing Body of the school will ensure that:

- There is a senior member of the school's leadership team who is designated to take the lead on e-learning/safety within the school (the headteacher).
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

4. **TEACHING AND LEARNING**

Benefits of internet use for education:

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and pupils and benefits education by allowing access to world - wide educational resources including art galleries and museums as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority and the DfE.

4.4 The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.
4.5 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the pupils.
4.6 Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
4.7 Pupils will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Pupils will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.
4.8 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. **MANAGING INTERNET ACCESS**

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include setting up a robust firewall and then monitoring and filtering access, appropriate to the age of the pupils.
5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. They will be aware of how the internet is monitored in school. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.
5.3 Pupils will be taught and know what to do if they experience material that they find distasteful, uncomfortable or threatening.
5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the e-learning designated lead.
5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6. **MANAGING E-MAIL**

6.1 Personal e-mail or messaging between staff and pupils should not take place.
6.2 Staff must use their school e-mail address or the school's email address if they need to communicate with parents of pupils.
6.3 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole class or group e-mail addresses should be used at KS1 and below.

6.4 Pupils must not reveal details of themselves or others in any email communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.
6.5 Access in school to external personal e-mail accounts may be blocked.
6.6 E-mail should be authorised by the class teacher before sending to an external organisation just as a letter written on school headed note-paper would be.
6.7 The forwarding of chain letters is not permitted.
6.8 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

7. **MANAGING WEBSITE CONTENT**

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
7.2 Photographs of pupils will not be used without the written consent of the pupil's parents/carers.
7.3 Pupils' full names will not be used anywhere on the web site, particularly in association with photographs.
7.4 The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.
7.5 Use of photographs on the school website will be carefully selected so that individual pupil's photographs will not be on the main school website, so that images of individuals cannot be misused.
7.6 The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupil's home information will not be published.
7.7 The Headteacher will have overall editorial responsibility and ensure that all content is accurate and appropriate both on the school website.
7.8 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

8. **SOCIAL NETWORKING AND CHAT ROOMS**

8.1 The school will block access to social networking sites.
8.2 Newsgroups will be blocked unless a specific use is approved.
8.3 Pupils will be advised never to give out personal details of any kind which may identify them or their location.
8.4 Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

9. **MOBILE PHONES**

9.1 Mobile phones will not be used by staff or pupils during school hours or during after school events.
9.2 Staff will ensure that when phones are used during breaks, they do so in areas where children are not present.

10. **FILTERING AND MONITORING**

10.1 The School will work in partnership with parents/carers; the Local Authority, Governors, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed, in place and improved regularly.
10.2 Within school, our Designated Safeguarding Lead is in charge of monitoring and filtering. Staff, pupils and Governors are aware of this and understand the role they play in keeping the school safe.
10.3 If staff or pupils discover unsuitable sites, the URL and content must be reported to the Headteacher, Designated Safeguarding Lead or the Deputy Safeguarding Lead.
10.4 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).
10.5 School will log any Smoothwall breaches, with actions and outcomes, and ensure that the filtering and monitoring is robust in school.
10.6 Regular checks by senior staff will ensure that the filtering methods selected are appropriate, effective and reasonable.
10.7 Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

11. **AUTHORISING INTERNET ACCESS**

11.2 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.
11.3 The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.
11.4 Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's Home-School Internet User Agreement document and give permission for their child to access ICT resources.
11.5 Staff will supervise access to the internet from the school site for all pupils.

12. **PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY**

12.1 It is not appropriate to use photographic or video technology in changing rooms or toilets.

12.2 Staff may use photographic or video technology to support and capture learning on school trips and appropriate curriculum activities.
12.3 Audio and video files may not be downloaded without the prior permission of the Headteacher.
12.4 Pupils must have permission from a member of staff before making a video or audio recording in school or on educational activities.
12.5 Webcams may be used with the permission of the Headteacher.

ASSESSING RISKS

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences of internet access.
13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.
13.4 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.
13.5 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.
13.6 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14. INTRODUCING THE POLICY TO PUPILS

14.1 Rules for internet access will be posted in all rooms where computers are used.
14.2 Responsible internet use, covering both school and home use, will be included in the PSHE curriculum and as part of an E-Safety Week or Day and each computing unit will revisit E-safety as part of the learning.
14.3 Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet. They will be confident and have a clear

understanding of the Child Exploitation and Online Protection (CEOP) weblink/button. This will form part of the PSHE curriculum.
14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.
14.5 Digital leaders are trained by staff to support the delivery of E-safety during Safer Internet Day/Week, and to support the general use of ICT and computing within the school day.

15. **CONSULTING STAFF**

15.1 It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff will be provided with a copy of the school's E-Safety Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- The head teacher and Key Stage leaders will supervise members of staff who operate the monitoring procedures.

16. **MAINTAINING ICT SECURITY**

16.1 Personal data sent over the network will be encrypted or otherwise secured.
16.2 Teachers files will not be able to be accessed by pupils when logged in using the class page and password.
16.3 The Headteacher in partnership with the school's ICT consultancy will ensure that the system has the capacity to deal with increased traffic caused by internet use.

17**. DEALING WITH COMPLAINTS**

17.1 Staff, pupils, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must dealt with through the school's Safeguarding Policy and Procedures.
17.2 The Headteacher is the school's designated person for e-safety and will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Headteacher immediately.
17.3 Pupils and parents/cares will be informed of the complaints procedure.
17.4 Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

17.5 As with drugs issues, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.
17.6 Sanctions for misuse may include any or all of the following:

- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time
- Referral to the police.

18. PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's Internet Policy and E-Safety Policy which may be accessed on the school website.
18.2 Any issues concerning the internet will be handled sensitively to inform parents/cares without undue alarm.
18.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.
18.4 Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).
18.5 A partnership approach will be encouraged with parents/carers and this may include practical sessions as well as suggestions for safe internet use at home.
18.6 Parents will be invited to a Parent Internet Safety Talk which will be held every two years or sooner if the need arises.