Stamfordham Primary School

E-Safety Policy

Reviewed by ES (Computing lead): June 2022
Approved by LB (Head): June 2022
Approved by Governors: May 2021

Due for review: July 2023

1 INTRODUCTION

1.2 This policy has been developed to ensure that all adults in Stamfordham Primary School are working together to safeguard and promote the welfare of children and young people. This policy has been ratified by the Governing Body and will be reviewed annually.

1.3 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.

1.4 This document aims to put in place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of 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 children, young people and staff from risks and infringements.

1.5 The Head Teacher/SLT or, in their absence, the authorised member of staff for e-safety, Emily Snowball, Computing Co-ordinator, has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.6 This policy complements and supports other relevant school and Local Authority policies.

1.7 The purpose of internet use in school is to help raise educational standards, promote pupil achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

1.8 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

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. The Keeping Children Safe in Education 2020 document sets out the legal duties that must be followed to safeguard and promote the welfare of children and young people under the age of 18 in schools and refers to online safety.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 teach and support e-safety practices in school, 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 is not limited to school premises, school equipment or the school day. This means that we will intervene in incidents that also occur outside of school if bought to our attention.

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 be dealt with in accordance with the school's Anti-Bullying and Code of Conduct 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 Head Teacher of Stamfordham Primary School 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.
- A Designated Member of Staff for E-Safety (ES) is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E-Safety Policy and arrangements.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. 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-Safety within the school.
- 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 computing and e-safety training.

3.3 The Designated Members of Staff for E-Safety will:

- Act alongside HT as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received and signed a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and aware of the school's E-Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network and report any concerns to the designated person.

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 children 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. The internet plays a vital role for those staff and children isolating at home, although school will support families accommodating learning resources where needed.

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 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 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 children.

4.7 Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation and how to keep themselves safe online using SMART rules.

4.8 Children and young people 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. Children and young people will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 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 strict filtering appropriate to the age of the children.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Teaching 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 what to do if they experience material that they find distasteful, uncomfortable or threatening. Pupils will be directed to use the "cross" icon to close screens if needed. Child- friendly rules linked to the safe use of the internet will be displayed in each classroom and children will be encouraged to know and refer to them when needed (SMART rules).

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Local Authority via the Computing Co-ordinator/HT.

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 must not take place.

6.2 Pupils and staff may only use approved school 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 only be used at KS2 for home learning. The teacher will manage these temporary accounts and pupils will only be able to contact each other in a controlled environment for purposes of lessons.

6.3 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.4 Access in school to external personal e-mail accounts may be blocked.

6.5 Excessive social e-mail use can interfere with learning and will be restricted.

6.6 The forwarding of chain letters is not permitted.

6.7 Incoming e-mail should be monitored and attachments by staff members should not be opened unless the author is known.

6.8 All staff emails sites must be closed during lessons and should not be displayed on the screen for children to see.

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. Parents/carers will be issued with a consent form for this purpose when their child initially enters school (Admin to update list annually/or when new child arrives).

7.3 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.

7.4 The Head Teacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 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.

7.6 Use of site photographs will be carefully selected so that pupils cannot be identified or their image misused.

7.7 Only the first names of pupils will be used on the website, particularly in association with any photographs. Any breach of this will be reported immediately to the DPO.

7.8 Work will only be used on the website with the permission of the pupil and their parents/carers.

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8 SOCIAL NETWORKING AND CHAT ROOMS

8.1 The school will control access to moderated social networking sites and educate pupils in their safe use.

8.2 The Class Dojo site will be used by staff and parent/carers to communicate and share class and school information, news, photos and behaviour rewards. Access is controlled with passwords. Class dojo will be used in the event of remote learning (see Remote learning Policy).

8.3 Staff in the Early Years will use the online assessment tool "Tapestry" to share attainment and achievement of pupils in nursery and reception with their parent/carers through photos, videos and written observations. Secure passwords are used for parent/carers to access this.

8.4 Pupils will not access social networking sites e.g. ''Facebook' or 'Twitter' whilst at school.

8.5 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms, games and apps.

8.6 Pupils will not be allowed to access public or unregulated chat rooms.

8.7 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.8 Newsgroups will be blocked unless an educational need can be demonstrated.

8.9 Pupils will be advised to use nick names and avatars when using social networking sites as opposed to using their personal information.

8.10 Pupils will be advised never to give out personal details of any kind which may identify them or their location.

8.11 Pupils should be advised not to place personal photos on any social network space.

8.12 Pupils should be advised on security and encouraged to set passwords, deny access to unwanted individuals or and instructed how to block unwanted communications.

8.13 Pupils should be encouraged to invite known friends only and deny access to others.

8.14 Pupils and parents should be made aware that some social networks, APPS and games are not appropriate for children of Primary age.

8.15 Staff will not exchange social networking addresses or use social networking sites to communicate with pupils.

8.16 Pupils will be advised to be selective about the photographs they choose to share on social networking apps and websites such as “facebook” and “snap chat”. Work will be done with all pupils in PHSCE to help them to understand the possible consequences of sharing personal or explicit photographs with others and that some photos are permanent. Through this work, they will develop an understanding of their “digital footprint”.

8.17 Pupils and parents must be aware that certain games and apps are not appropriate for the age of primary school children , and be advised to adhere to the PEGI rating.

9 MOBILE PHONES

9.1 Mobile phones will be allowed by staff members. Phones must be kept in bags or lockers at all times and staff should not access their phones during lesson time. The sending of abusive or inappropriate text messages or files by any means is forbidden and will be dealt with in accordance with the school’s Anti-Bullying and Behaviour Policies.

9.2 Staff who intend to use personal mobile phones or other mobile technology to access their school email, must ensure that their device is encrypted with a personal password, PIN or fingerprint recognition. Passwords and personal information relating to personal devices should be kept confidential.

9.3 Staff should not, under any circumstances take photographs in school using their mobile phone. They must not use their mobile phones on school trips to take photographs.

9.4 Mobile phones will not be allowed by pupils in school. However, some pupils may need to have a mobile phone for safety reasons so that they are able to contact their parent/carer and vice versa. e.g. when walking to and from school alone. In these circumstances, mobile phones may be brought to school by pupils and left, turned off, in the school office for safe keeping. The use of mobile phones in any area of school or during lessons is strictly prohibited.

9.5 Pupils will be advised to carefully consider the items they share via mobile phones such as photos and texts. The possible negative impact of “sexting” or sharing personal or

explicit photographs with others through apps accessible via mobile phones will be addressed in PSHCEE and e-safety lessons.

9.6 Parent/carers must not use their mobile phones within school, this includes taking pictures.

10 FILTERING

10.1 The school will work in partnership with parents/carers; the Local Authority, the DfE and the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly – firewall system in place.

10.2 If staff or pupils discover unsuitable sites, the URL and content must be reported to the E-Safety lead and appropriate measures will be taken to ensure safety.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk) by the E-Safety co-ordinator.

10.4 Regular checks by MGL and Computing lead will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

10.6 For the purposes of teaching and learning, selected members of teaching staff will be trained in how to adjust filters for a brief period to access specific sites needed for certain lessons. MGL and Computing lead will support staff in enabling this. Teaching staff must fully explore these sites before allowing pupils access, monitor pupils closely and make pupils aware of their responsibility in relation to making sensible choices about what they access while online. Filters will only be adjusted with good reason for purpose.

11 AUTHORISING INTERNET ACCESS

11.1 All staff must read and sign the school's 'Staff Code of Conduct for ICT' before using any school ICT resources and any staff not directly employed by the school will be asked to sign the school's 'Acceptable Use' policy document before being allowed internet access from the school site.

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 'Acceptable Use' 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.

11.6 All pupils in Reception through to year 6 must sign the child-friendly Acceptable usage of ICT policy at the start of each academic year and also pupils who arrive at different points

in the year will complete the child-friendly acceptable use of ICT policy at their induction meeting. The acceptable use policy, outlines clear rules for the use of equipment within school.

12 PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

12.1 When not in use all video conferencing cameras will be switched off and turned towards the wall.

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

12.3 Staff may use photographic or video technology to capture school trips and support appropriate curriculum activities. Staff must not use their own devices for this.

12.4 Audio and video files may not be downloaded without the prior permission of the network manager.

12.5 Pupils must have permission from a member of staff before making or answering a videoconference call or making a video or audio recording in school or on educational activities.

12.6 Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

12.7 images, audio and video taken on Ipad devices must be kept secure with the school's username and password.

12.8 Images and videos taken on ipads will be deleted on a half termly basis by the School support technician and Computing lead

13 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 Head Teacher 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.

13.7 A designated person will complete an annual e-safety review to ensure that appropriate measures are in place.

14 INTRODUCING THE POLICY TO PUPILS

14.1 SMART 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 and Computing curriculum.

14.3 An annual Safer Internet Day will be held in school to develop awareness of e-safety amongst pupils.

14.4 E-safety will be a key part of a progressive curriculum that is flexible, relevant and engages pupils interest. The ICT/Computing curriculum will be used to promote e-safety through teaching pupils how to protect themselves from harm and how to take responsibility for their own and others safety.

14.5 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.

14.6 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

14.7 Positive sanctions will be used to reward positive and responsible use.

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 are governed by the terms of the school's 'Staff Code of Conduct for ICT' and will be provided with a copy of the Acceptable Use 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.
- Senior managers 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 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

16.3 USB drives that are used with school technology must be encrypted to maintain security and prevent viruses. Any USB drive that is not encrypted must not be used under any circumstances, including those used by outside agencies.

16.4 Child accounts will be blocked from using personal USB drives.

MAINTAINING SECURITY FOR REMOTE LEARNING

16.5 All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

16.6 Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)

16. 7 Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

16.8 Making sure the device locks if left inactive for a period of time

16.9 Not sharing the device among family or friends

16.10 Installing antivirus and anti-spyware software and Keeping operating systems up to date – always install the latest updates

17 DEALING WITH COMPLAINTS

17.1 Staff, children and young people, parents/carers must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures. Staff may record incidents using the school CPOM system.

17.2 The school's Head Teacher will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Head Teacher immediately.

17.3 Pupils and parents/carers 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 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, which may ultimately prevent access to files, held on the system, including examination coursework.
- Referral to the police.

18 PARENTS/CARERS SUPPORT

18.1 Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website.

18.2 Any issues concerning the internet will be handled sensitively to inform parents/carers 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 Parent/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP) and the NSPCC site SHAREAWARE and NETAWARE. A link to this will be available on the school website.

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 involved in the annual Safer Internet Day Materials, advice will be shared through class assemblies, information sessions and workshops. Parent/carer questionnaires will be completed to increase e-safety awareness. Analysis of these questionnaires will be used to inform any future support needed.

19 COMMUNITY USE

19.1 School ICT resources may be increasingly used as part of the extended school agenda.

19.2 Adult users will sign the school's acceptable use policy.

19.3 Parents/carers of children and young people under 16 years of age will be required to sign the acceptable use policy.

19.4 Any visitors to school will agree to the acceptable usage policy on signing in.

20 SAFEGUARDING & REMOTE LEARNING

20.1 With the increased use of digital technologies that comes with remote learning, safeguarding implications need careful consideration.

20. 2 Parents are advised to spend time speaking with their child(ren) about online safety and reminding them of the importance of reporting to an adult anything that makes them feel uncomfortable online. While we will be doing our best to ensure links shared are appropriate, there may be tailored advertising which displays differently in your household or other changes beyond our control.

20.3 Online safety concerns should still be reported to the child's class teacher and school's Online Safety Lead (ES) as normal. Parents can do this through Class Dojo messaging or by phoning the school office.

20.4 The following websites offer useful support:

•Childline - for support
•UK Safer Internet Centre - to report and remove harmful online content
•CEOP - for advice on making a report about online abuse
In addition, the following sites are an excellent source of advice and information:
•Internet matters - for support for parents and carers to keep their children safe online
•Net-aware - for support for parents and careers from the NSPCC

•Parent info - for support for parents and carers to keep their children safe online
•Thinkuknow - for advice from the National Crime Agency to stay safe online

20. 5 If parents have any online safety concerns that need discussing, they can contact us through the usual channels and one of our Safeguarding Leads will get in touch.

20.6 Staff should continue to be vigilant at this time and follow our usual online safety and safeguarding / child protection policies and procedures, contacting a safeguarding lead directly by phone in the first instance.

……

I acknowledge receipt of the school's Policy for E-Safety

Name ..Miss Snowball……

Signed: ...E.Snowball…….. Date: ...11.05.21……..