New Swannington Primary School

E-Safety Policy

Approved by Governors: 01/07/25
Issue Date: 23/09/26

Next Review Date	Actual Review Date	Reviewed By	Changes made to Policy	Date & Minute No.	Chair of Governors Signature
Sept 2025	1/7/25	GB	None	1/7/25	A Cave
Sept 2026	27/10/26	GB	H/T	27/10/26	A Cave

E-Safety Policy

1. Introduction

2. Scope of Policy

3. Policies and Practices

    3.1 Use of internet facilities, mobile and digital technologies
    3.2 Reporting abuse

4. Education and Training

5. Infrastructure and Technology

    5.1 Partnership working

6. Inspection and Standards

    6.1 Monitoring
    6.2 Sanctions

7. Working in partnership with Parents and Carers

8. Associated Policies

1. Introduction

1.1 New Swannington Primary School recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at New Swannington Primary School want to ensure that the internet and other digital technologies are used to:

- raise educational standards and promote pupil achievement;
- develop the curriculum and make learning exciting and purposeful;
- enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen, we have taken a whole school approach to E-safety as promoted by British Education Communication Technology Agency (BECTA), which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's ICT infrastructure and technologies.

1.3 New Swannington Primary School, as part of this policy, holds steadfastly to the ethos that there should be an equitable learning experience for all pupils using ICT technology. We recognise that ICT can allow children with additional needs increased access to the curriculum and other aspects related to learning.

1.4 New Swannington Primary School is committed to ensuring that **all** its pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

1.5 The nominated senior person for the implementation of the School's E-safety policy is Mrs Palumbo.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 New Swannington Primary School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using the internet and other digital technologies;
- adequate training for staff and volunteers;
- adequate supervision of pupils when using the internet and digital technologies;
- education that is aimed at ensuring safe use of internet and digital technologies;
- a reporting procedure for abuse and misuse.

3. Policies and Procedures

New Swannington Primary School understand that effective policies and procedures are the backbone to developing a whole-school approach to E-safety. The policies that exist with New Swannington Primary School are aimed at providing a balance between exploring the educational potential of new technologies and providing safeguards to pupils.

3.1 Use of internet facilities, mobile and digital technologies

3.1.1. New Swannington Primary School will seek to ensure that internet, mobile and digital technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

3.1.2 New Swannington Primary School expects all staff and pupils to use the internet, mobile and digital technologies responsibly and strictly according to the Acceptable Use Policy. These expectations are also applicable to any voluntary, statutory and community organisations that makes use of the school's ICT facilities and digital technologies.

Users shall not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - indecent images of children;
    - promoting discrimination of any kind;
    - promoting racial, religious or homophobic hatred;
    - promoting illegal acts;
    - any other information, which may be offensive to peers or colleagues.

3.1.3 The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded so that it can be justified if required.

3.1.4 Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative);
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist or anti-religious material;
- violence and bomb making;
- illegal taking or promotion of drugs;
- software piracy;
- other criminal activity.

3.1.5 In addition, users may not:

- use the Sophos' facilities for running a private business;
- enter into any personal transaction that involves Sophos or member Local Authorities in any way;
- visit sites that might be defamatory or incur liability on the part of Sophos or member Local Authorities or adversely impact on the image of Sophos;
- upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of Sophos, or to Sophos itself;

- reveal or publicise confidential or proprietary information, which includes but is not limited to:
  - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorized access to facilities or services accessible via Sophos or equivalent broadband provider
- Undertake activities with any of the following characteristics:
  - wasting staff effort or networked resources, including time on end systems and the effort of staff involved in support of those systems;
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
  - using the school network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
  - continuing to use an item of networking software or hardware after the network has requested that use cease because it is causing disruption to the correct functioning the network;
  - other misuse of the network, such as introduction of viruses.
- Use mobile technologies 3G, 4G or mobile internet services in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

3.2 Reporting Abuse or Inappropriate Content

The following outlines the procedures to undertake if a child or adult receives an abusive email or accidentally accesses a website that contains abusive or inappropriate material.

Children who come across inappropriate content should:

- turn off the monitor if using a desktop computer. Cover the screen of a mobile device and/or take a screen shot of the inappropriate page;
- know not to close the screen/page containing the content so that an adult who is in the room can see the nature of the content to report it;
- immediately tell an adult who is in the room about what has happened. Adults look at nature of content (if appropriate) and report incident to the Headteacher.

Adults who come across inappropriate content should:

- make a note of search term used (if using a search engine) or what they were doing online at the time when they came across the inappropriate content;
- report immediately to the Headteacher if using the internet in school or report as soon as possible after the incident if using a school laptop or device at home.

4. Education and Training

4.1 New Swannington Primary School recognises that the internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

4.2 As part of achieving this, we want to create within New Swannington Primary School an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely.

4.3 To this end, New Swannington Primary School will:

- enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum;
- educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem;
- support parents in gaining an appreciation of internet safety for their children and provide them with relevant information on the policies and procedures that govern the use of internet and other digital technologies within the school.

4.4 At New Swannington Primary School, e-safety education is delivered in the following ways:

- as a discrete subject;
- as part of the wider curriculum, embedded within other subjects;
- through assemblies, with the support of the pupil e-safety committee.

5. Infrastructure and Technology

5.1 Partnership working

5.1.1 New Swannington Primary School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is SOPHOS (Our internet Service Provider). As part of our commitment to partnership working, we fully support and will continue to work with SOPHOS to ensure that pupil and staff usage of the internet and digital technologies is safe.

5.1.2 New Swannington Primary School will, as part of its wider safeguarding responsibilities, seek to ensure that voluntary, statutory and community organisation take an approach to their activities that sees the welfare of the child as paramount. To this end, we expect any organisation using the school's ICT or digital technologies to have appropriate policies and procedures that are aimed at safeguarding children and young people and reporting concerns.

6. Inspection and Standards

New Swannington Primary School recognises the need to have regular inspections of policies and procedures to ensure that its practices are effective and that the risks to pupils are minimised.

6.1 Monitoring and online safety

6.1.2 Our school approach to online safety, including appropriate filtering and monitoring on school devices and school networks is reflected in this Child Protection Policy including awareness of the ease of access to mobile phone networks. (See KCSiE 2026 Paragraph 138).

6.1.3 Our Senior DSL and the DSL team has the lead responsibility in this area, which is overseen and regularly reviewed by the Governing body/ trust, along with considering the number of and age range of

their children, those who are potentially at greater risk of harm, and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

6.1.4 Our Governing body will ensure they maintain oversight of the Online Safety Policy contained within our main child protection policy, and the arrangements put in place to ensure appropriate filtering and monitoring on school devices and school network. The appropriateness of any filtering and monitoring systems will in part be informed by the risk assessment required by the Prevent Duty as required by KCSiE 2026 paragraph138 to147.

This will include:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet the school safeguarding need.
- review and discuss the standards with the leadership team, IT staff and service providers to ensure the school/college meets the standard published by the Department for Education filtering and monitoring standards.

We receive weekly filtering reports from our ICT support provider on what is being accessed in school and where possible names of children are provided as well as date/times when sites are accessed.

Regularly test the filtering system via Test Your Internet Filter | SWGfL Test Filtering

Regularly check pupil/staff devices to ensure the correct filters are applied and random testing to check inappropriate content is being blocked.

Senso.cloud | Cloud-Based Device Monitoring and Management system has been introduced to allow for advanced reporting on what pupils are accessing, AI driven threat analysis, instant alerts to DSL's and integration with CPOMS so escalated violations or concerns can be directly imported.

Our Governing body/trust will ensure a review is maintained to ensure standards. They will discuss with IT staff and service providers these standards and whether more needs to be done to support our school/college in meeting and maintaining these standards and communicating these to staff, our pupils, parents, carers and visitors to the school who provide teaching to children as part of the learning and educational opportunities we provide.

Our Senior DSL and the DSL team will always act in the 'best interest of the child' and remain mindful of the importance with parents and carers about safeguarding concerns held for children and in particular children's access to online sites when away from school.

We will support understanding of harmful online challenges and hoaxes and share information with parents and carers and where they can get help and support.

6.2 Sanctions

6.2.1 New Swannington Primary School has been careful to develop in conjunction with its partners, policies and procedures to support the innocent in the event of a policy breach and enable the School to manage such situations in, and with, confidence.

6.2.2 Where there is inappropriate or illegal use of the internet and digital technologies, the following steps will be taken:

- Child / Young Person
  - The child/young person will be spoken to and support will be provided and (if deemed appropriate) the Behaviour policy of the school will be applied.
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

- Adult (Staff and Volunteers)
  - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy.
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

6.2.3 If inappropriate material is accessed, users are required to immediately report this to Mrs Palumbo, Headteacher and Sophos so this can be taken into account for monitoring purposes.

7 Working in Partnership with Parents and Carers

7.1 New Swannington Primary School is committed to working in partnership with parents and carers and understand the key role they play in the internet safety of their children through promoting internet safety at home and elsewhere.

7.2 New Swannington Primary School also appreciate that there may be some parents who are concerned about the use of the internet, email and other digital technologies in school. In such circumstances, school staff will meet with parents and carers to discuss their concerns and, if necessary, agree upon a series of alternatives that will allow their child to fully access the curriculum, whilst remaining safe. Parents will receive further support and information via updates on the school newsletter, school website and through letters and leaflets sent home.

8 Associated Policies

8.1 There are multiple aspects of the school's E-safety policy, which include acceptable use policies for both staff and pupils; ICT equipment (onsite and offsite); data security and retention. The various policy documents relating to these aspects of the school's E-Safety Policy can be obtained from Mrs Palumbo, Headteacher for scrutiny, if required.