PADNELL INFANT SCHOOL

BOARD OF GOVERNORS

E-SAFETY POLICY

Name of Unit/Premises/Centre/School	Padnell Infant School
Date of Policy Review	February 2026
Date of Next Review	February 2028
Name of Headteacher	Mrs Mandy Grayson

Administration Record

Issue	Modification	Approved
1	For FGB Approval	17 September 2018
1.1	FGB Comments Incorporated - Approved	24 September 2018
2	FGB Approval	2 March 2020
3	FGB Approval	7 March 2022
4	FGB Approval	26 February 2024
5	FGB Approval	February 2026

Contents Page

Administration Record **2**
Contents Page **3**
1 Introduction **4**
2 IT Vision **4**
3 Definition **4**
4 E-Safety Coordinator **4**
5 Teaching and Learning **4**
5.1 Importance of the internet and digital communications 4
5.2 Internet Use to Enhance Learning 5
5.3 Pupils will be taught how to evaluate internet content 5
6 Managing Internet Access **5**
6.1 Information System Security 5
6.2 E-Mail 5
6.3 Published Content and School Website 6
6.4 Publishing Pupil's Images and Work 6
6.5 Chat and Instant Messaging 6
6.6 Photographic, Video and Audio Technology 7
6.7 Emerging Technologies 7
7 Policy Decisions **8**
7.1 Authorising Internet Access 8
7.2 E-Safety Complaints 8
7.3 Risk Assessment 8
7.4 Filtering 9
8 Communication of the e-safety **9**
8.1 To pupils 9
8.2 To staff 10
8.3 To parents 10

1 Introduction

1.1.1 This policy should be read in conjunction with our Internet Access Policy, Behaviour and Rewards and Anti-Bullying Policies.

1.1.2 This policy has been written by the school, building on the Kent E-Safety Policy and government guidance. It has been agreed by senior management and approved by the Governors.

2 IT Vision

2.1.1 At Padnell Infant School our vision for Information Technology (IT) is that the children will learn the necessary skills to be able to use IT as a useful learning tool, integrated across the curriculum. Teaching staff will have the skills to use IT as a teaching tool to enhance the children's learning.

3 Definition

3.1.1 E-Safety encompasses Internet technologies and electronic communications such as mobile phones and watches. It highlights the need to educate pupils about the rights and responsibilities of using technology and provides safeguards and awareness for users to enable them to control their online experience.

4 E-Safety Coordinator

4.1.1 The E-Safety coordinators are Mrs Lisa Kernot who is the IT curriculum lead and Mrs Tarryn Rowe who is the IT lead across the school supported by Agile. Mrs Grayson, the Headteacher also takes a wider responsibility for E-Safety and this role will be undertaken in conjunction with that of the Designated Safeguard Lead.

5 Teaching and Learning

5.1 Importance of the internet and digital communications

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.

5.2 Internet Use to Enhance Learning

- The school internet access will be designed expressly for pupil use and will include filtering and monitoring systems 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.

5.3 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 will be taught the importance of cross-checking information before accepting its accuracy;
- Pupils will be taught to report any unpleasant internet content to a member of staff. They understand to use the cross to close any screen and use our song to remind them to stop and think before they 'tap or click' and 'tell someone' if anything feels wrong or uncomfortable.

6 Managing Internet Access

6.1 Information System Security

- School IT systems security will be reviewed regularly;
- Virus protection will be updated regularly.

6.2 E-Mail

- Any offensive e-mails received by staff must be reported immediately to one of the coordinators;
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known;
- The forwarding of chain letters is not permitted;

- Staff will use their school email and not a personal one for school business; however, parent communication should be via the office email to help protect wellbeing and promote quality of communication.

- Governors will use their school e-mail address when sensitive information is being distributed.

6.3 Published Content and School Website

- Staff and pupil personal contact information will not be published. The contact details given online will be those of the school admin team;

- The Headteacher will take overall responsibility and ensure that content is accurate and appropriate.

6.4 Publishing Pupil's Images and Work

- Written permission will be obtained from parents and carers before photographs of any child are published on the internet, either through the school website or any external website;

- Pupil's full names will not be used anywhere on the website, particularly in association with photographs.

6.5 Chat and Instant Messaging

- Pupils will not be allowed access to any chat rooms that are not securely monitored. Any that are used as part of the curriculum will not be accessible by the public and will require approval before comments are posted. E.g.Purple Mash and See-Saw;

- Pupils will not access social networking sites for example 'Instagram', 'Facebook' or 'Snapchat';

- Any form of bullying or harassment is strictly forbidden in accordance with our anti-bullying policy;

- When publishing material to websites and elsewhere, pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.

- **This statement relates to an employment tribunal decision:**
  Under normal circumstances, no member of staff should engage in direct communication (in or out of school) of a personal nature with a pupil who is not a member of their direct family, by any means, for example (but not limited to) SMS text message, e-mail, instant messaging or telephone, Facebook or Snapchat. Should special circumstances arise where such communication is felt to be necessary, the agreement of the Headteacher should be sought first and appropriate professional language should always be used.

6.6 Photographic, Video and Audio Technology

- Videoconferencing and webcam use will be appropriately supervised for the pupils' age;
- No recording should be taken using any personal devices such as mobile phones or watches. Children are not permitted to have any phones or watches with a recording element or gaming aspect in school. Should these be in school they will be removed and an adult will be asked to come and collect the device at the end of the school day.
- It is not appropriate to use photographic or video devices in changing rooms or toilets and care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed;
- Staff may use school iPads to support school trips and curriculum activities; they should be cleared before leaving the school site in case of being misplaced.
- The downloading of audio or video files is permitted. However, staff should be made aware of licensing regulations and ensure the content is age appropriate. Any downloads must be viewed or listened to fully before sharing with the children and relate directly to the current educational task being undertaken.

6.7 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed;
- Staff should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Pupils will not be allowed to use mobile phones, personal iPads or smart watches of any kind in school;

- Games machines including Playstation, Xbox and Nintendo Switch have internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

7 Policy Decisions

7.1 Authorising Internet Access

- All staff and pupils are granted internet access. A list will be kept of any pupil who has this access withdrawn;
- Access to the internet will be by adult demonstration with occasional directly supervised access to specific approved on-line materials. Shortcuts to websites that will be of educational value to the pupils will be placed on the learners desktop in order that children may access them directly and minimise the use of search engines. The school website will be the home page and access will be encouraged via this as much as possible.
- A child-friendly search engine will be promoted at all times.

7.2 E-Safety Complaints

- Pupils and parents will be informed of consequences for pupils misusing the internet. Sanctions available include:
  - *i) Informing Parents or Carers;*
  - *ii) Interview and counseling by Headteacher;*
  - *iii) Removal of internet or computer access for a period.*
- Complaints of internet misuse by pupils will be dealt with by the Headteacher. Any complaint about staff misuse must be referred to the Headteacher.

7.3 Risk Assessment

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990;
- Methods to identify, assess and minimise risks will be reviewed regularly;

- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored;
- Access is strictly forbidden to any websites that involve gambling or financial scams.

7.4 Filtering

- The school will work in partnership with parents; the Local Authority, Department for Education and our Internet Service Provider 'Agile', to ensure systems to protect pupils are reviewed and improved;
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT Leader;
- In accordance with KCSiE 2023, Agile will review the access reports and feedback to the Headteacher/DSL and IT Leader any concerns. The reports will be signed and filed in the office. This will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable;
- Any harmful or inappropriate content will be blocked, without unreasonably impacting on teaching and learning (KCSiE 2023)
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.org.uk);
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupils.

8 Communication of the e-safety

8.1 To pupils

- E-Safety rules will be written in conjunction with the school council and will be posted in all rooms where computers are used. They will be discussed with pupils regularly, especially when using the internet;
- Assemblies will promote the safe use of IT equipment;
- The child section on the school website will contain a suitable link to promote safety awareness.

8.2 To staff

- All new staff will be made aware of this policy and be taken through the key parts as part of their induction. This will be signed and refreshed annually;
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential;
- The monitoring of internet use is a sensitive matter. Members of staff who operate monitoring procedures will be supervised by senior management;
- Breaching this E-Safety Policy may result in disciplinary action being taken and access to IT being restricted or removed.

8.3 To parents

- Parents will be notified of the E-Safety Policy in newsletters and on the school website and via specific letters targeting issues as they arise;
- School encourages parental engagement with online safety through annual presentations and workshops to advise them thus promoting e-safety to the community;
- School sends out regular advice sheets produced by Knowsley City Learning Centres with information for families about how to keep their children safe when online. School also uses it's regular newsletter to remind parents of the dangers of accessing inappropriate content and how to monitor their children's use of devices.
- A partnership approach with parents will be encouraged;
- Parents of children who are showing signs of accessing inappropriate content at home will be contacted individually by the Headteacher and/or the Safeguarding Governor.