



# **PARKLANDS INFANT AND NURSERY SCHOOL**

## **Online Safety and Acceptable Use (for Children) Policy**

Approved by the Governing Body of Parklands Infant & Nursery School

Date: October 2024

Signed: \_\_\_\_\_

Mrs K Merriman (Chair of Governors)

## **Online Safety and Acceptable Use (for Children) Policy**

1. Introduction
2. Aims
3. Using the Internet for learning
4. Teaching safe use of the Internet and ICT
5. Access for all pupils
6. Suitable material
7. Non-education materials
8. Filtering and monitoring
9. Expectations of pupils using the Internet
10. School Website and Class Dojo

## **1. Introduction**

Computing in the 21st Century has an all-encompassing role within the lives of children and adults. New Internet and online technologies are enhancing communication and the sharing of information. We believe it is our responsibility to prepare pupils for their lives in the modern world, and IT is an integral part of that world. As a school, we are committed to teaching pupils to use IT effectively and appropriately in all aspects of their education. The school's Computing resources are essential to the effective delivery of learning for children in their Computing and Online Safety lessons and across the curriculum, and to raise educational standards. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Our Online Safety and Acceptable Use Policy for pupils has been discussed with staff, agreed by the senior management and approved by Governors. It will be reviewed annually.

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use of IT, the Internet and Electronic Communication Policy (AUP)
- Code of Conduct policy
- Acceptable Use of Mobile phones, Mobile Devices, and Cameras
- Behaviour and Discipline policy
- Child Protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- GDPR policy

## **2. Policy Aims**

The aims of this Acceptable Use Policy for children are to:

- Ensure that all pupils benefit from all learning opportunities offered by the computing and Internet resources provided by the school in a safe and controlled manner.
- To give pupils clear guidance on safe and acceptable use of these resources.
- Make pupils are aware that Internet use in school is a resource and a privilege.

## **3. Using the Internet for learning**

The internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials. We teach all our pupils how to find appropriate information on the internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is. Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils.

- Teachers carefully plan all internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials
- Children are taught how to use search engines and how to evaluate internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught about misinformation on the internet.

#### **4. Teaching safe use of the Internet and IT**

We think it is crucial to teach pupils how to use the internet safely, both at school and at home. Teaching Online Safety happens continuously (and incidentally when required) in the classroom, during assemblies and PSHE lessons etc. Our Whole-School Online Safety Skills Document maps out specific and progressive content, which is taught across school throughout the year-

**see Appendix B.**

- Our 'Smartie the Penguin' statements in each classroom are 'child friendly' prompts to aid children when exploring and understanding life online.
- Children learn that not all content online is true, people may lie and not be who they say they are. Children know they can tell a parent/carer or someone they trust if someone or something makes you feel uncomfortable or worried.

#### **5. Access for all pupils**

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning.

#### **6. Suitable material**

We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

#### **7. Non-Education materials**

As well as internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information. When in school, pupils are supervised by an adult when using the Internet.

#### **8. Filtering and Monitoring**

Filtering and Monitoring is in effect on school devices and our school network. Staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training.

Our internet provider uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable

material to occasionally get past the filter. Despite the best efforts of Parklands Infant School and school staff, occasionally pupils may come across something on the Internet that they find offensive, unpleasant or distressing. All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary. Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined in this document. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

## **9. Expectations of Pupils using the Internet**

- At Parklands, we expect all pupils to demonstrate the values of the Parklands Person, particularly to be a Safe Parklands Person whilst using the internet. This applies to children being responsible for their own behaviour on the internet, just as they are anywhere else in school. This includes materials they choose to access, and the language they use.
- Pupils using the internet are expected to avoid deliberately seeking out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.

## **10. School Website and Class Dojo**

- The website is regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publications of children's learning on the web or Class Dojo will be decided by a teacher.
- Photographs and video focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.

## Appendix A



### Acceptable Use Policy – Pupils

**“Before you click, click, click, you need to think, think, think...and tell someone.”**

**I Promise** – to only use school technology for schoolwork that the teacher has asked me to do.

**I Promise** – not to look for or show other people things that may be upsetting.

**I will not** – use other people's work or pictures without permission to do so.

**I will not** – damage IT equipment, if I accidentally damage something I will tell my teacher.

**I will not** – share passwords with anybody. If I forget a password, I will let my teacher know.

**I will not** – share personal information online with anyone.

**I will not** – download anything from the Internet unless my teacher has asked me to.

**I will** – let my teacher know if anybody asks me for personal information.

**I will** – be respectful to everybody online; I will treat everybody the way that I want to be treated.

**I understand** – that some people on the Internet are not who they say they are, and some people can be unkind. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

**I understand** – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

**Signed (Parent):**

**Signed (Child):**

**Date:**



## Appendix B

### Whole-School Online Safety Skills



\*with Education for a Connected World, Project Evolve and Teach Computing links 23-24

<b>Whole School</b>	<p>Understand and sign Acceptable Use Policy (safe use of IT in school and at home)</p> <p>Online safety meeting for parents/carers Spring Term.</p> <p>Safer Internet Day – Computing lead provides all year groups with plans and activities for this day.</p> <p>Online bullying – collective worship focus -Education for a Connected World</p> <p>Online Safety Smartie the Penguin <a href="http://www.childnet.com/resources/smartie-the-penguin">http://www.childnet.com/resources/smartie-the-penguin</a></p> <p>Half-termly online safety assemblies</p> <p>Reminders on newsletters</p>					
	<b>Autumn 1</b>	<b>Autumn 2</b>	<b>Spring 1</b>	<b>Spring 2</b>	<b>Summer 1</b>	<b>Summer 2</b>
<b>Nursery</b>	<p>In Nursery, our team focus on ensuring our children are safe users of technology, both in and out of school. To do this, the team will use the Project Evolve resources as a foundation for building age-appropriate sessions, removing content where necessary, on areas that have been identified as needing teaching through conversations with all stakeholders, children, families and school staff. Nursery staff will also use Online Safety stories, written by authors to engage children about Online Safety, in an age-appropriate way.</p>					
<b>Reception</b>	<p>All aspects of computing are taught through the inclusion of devices/digital technology throughout continuous provision. Children are exposed to a range of devices including Bee-Bots, iPads, desktop PCs and cameras. Online Safety is taught once per half term and EFCW links are followed.</p>					
	<p>EFCW - Health, well-being and Lifestyle</p> <p>I can recognise, online or offline, that anyone can say 'no' - 'please stop' - 'I'll tell' - 'I'll ask' to somebody who makes them feel sad, uncomfortable,</p>	<p>EFCW - Online Reputation</p> <p>I can identify ways that I can put information on the internet.</p> <p>EFCW - Online Bullying</p> <p>I can describe ways that some people can be unkind online.</p>	<p>EFCW - Copyright and Ownership</p> <p>I know that work I create belongs to me.</p> <p>I can name my work so that others know it belongs to me.</p>	<p>EFCW - Privacy and Security.</p> <p>I can identify some simple examples of my personal information (e.g., name, address, birthday, age, location). I can describe who would be trustworthy to share this information</p>	<p>EFCW - Online Relationships</p> <p>I can recognise some ways in which the internet can be used to communicate.</p> <p>I can give examples of how I (might) use technology to communicate with</p>	<p>EFCW - Self-Image and Identity</p> <p>EFCW - Managing Online Information</p> <p>I can identify devices I could use to access information on the internet.</p> <p>I can talk about how to use the internet as a way of finding information online.</p>

	embarrassed or upset.  I can give some examples of these rules.			with; I can explain why they are trusted	people I know	EFCW - Online Bullying I can offer examples of how I think this can make others feel
	<b>Digital Literacy/Computer Science</b>	<b>Information Technology</b>		<b>Computer Science</b>		
<b>Year 1</b>	<b>Technology around us</b>  <b>EFCW - Health, well-being, and Lifestyle</b> I can explain rules to keep myself safe when using technology both in and beyond the home.	<b>Digital painting</b>  <b>EFCW - Online Reputation</b> I can recognise that information can stay online and could be copied. I can describe what information I should not put online without asking a trusted adult first <b>EFCW - Online Bullying</b> I can describe how to behave online in ways that do not upset others and can give examples.	<b>Moving a robot</b>  <b>EFCW - Copyright and Ownership</b> I can explain why work I create using technology belongs to me. I can say why it belongs to me (e.g., 'I designed it' or 'I filmed it').	<b>Grouping data</b>  <b>EFCW - Privacy and Security</b> I can explain how passwords are used to protect information, accounts and devices. I can recognise more detailed examples of information that is personal to someone (e.g., where someone lives and goes to school, family names). I can explain why it is important to always ask a trusted adult before sharing any personal	<b>Digital writing</b>  <b>EFCW - Online Relationships</b> I can give examples of when I should ask permission to do something online and explain why this is important. I can use the internet with adult support to communicate with people I know (e.g., video call apps or services). I can explain why it is important to be considerate and kind to people online and to respect their choices.	<b>Programming Animations</b>  <b>EFCW - Self-Image and Identity</b> I can recognize that there may be people online who could make someone feel sad, embarrassed or upset. If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult. I can trust and how they can help. <b>EFCW - Managing Online Information</b>

				information online, belonging to myself or others.	I can explain why things one person finds funny or sad online may not always be seen in the same way by others.	I can give simple examples of how to find information using digital technologies, e.g., search engines, voice activated searching. I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke. I know how to get help from a trusted adult if we see content that makes us feel sad, uncomfortable, worried or frightened.
--	--	--	--	--	---	--

<p><b>Year 2</b></p>	<p><b>Information Technology around us</b></p> <p><b>EFCW – Online Reputation</b> I can describe how anyone's online information could be seen by others. I know who to talk to if something has been put online without consent or if it is incorrect</p>	<p><b>Digital photography</b></p> <p><b>EFCW Health, well-being and Lifestyle</b> I can explain simple guidance for using technology in different environments and settings e.g., accessing online technologies in public places and the home environment.</p> <p>I can say how those rules/guides can help anyone accessing online technologies. EFCW - Online Bullying I can describe how to behave online in ways that do not upset others and can give examples. I can explain what bullying is, how people may bully others and how bullying can make someone feel. I can explain why anyone who experiences bullying is not to blame. I can talk about how anyone</p>	<p><b>Robot algorithms</b></p> <p><b>EFCW: Copyright and Ownership</b> I can recognise that content on the internet may belong to other people. I can describe why other people's work belongs to them.</p>	<p><b>Pictograms</b></p> <p><b>EFCW: Privacy and Security</b> I can explain how passwords are used to protect information, accounts and devices. I can recognise more detailed examples of information that is personal to someone (e.g., where someone lives and goes to school, family names). I can explain why it is important to always ask a trusted adult before sharing any personal information online, belonging to myself or others. I can explain and give examples of what is meant by 'private' and 'keeping things private'. I can describe and explain some rules for keeping personal information private (e.g., creating and protecting passwords). I can explain how some people may have devices in their</p>	<p><b>Programming quizzes</b></p> <p><b>EFCW - Managing Online Information</b> I can use simple keywords in search engines I can demonstrate how to navigate a simple webpage to get to information I need (e.g., home, forward, back buttons; links, tabs and sections). I can explain what voice activated searching is and how it might be used, and know it is not a real person (e.g., Alexa, Google Now, Siri). I can explain the difference between things that are imaginary, 'made up' or 'make believe' and things that are 'true' or 'real'. I can explain why some information I find online may not be real or true.</p> <p><b>EFCW - Online Relationships</b> I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky (e.g., email, online gaming, a pen-pal in another school/country). I can explain who I should ask before sharing things about myself or others online. I can describe different way to ask for, give, or deny my permission online and can identify who can help me if I am not sure. I can explain why I have a right to say 'no' or 'I will have to ask someone'. I can explain who can help me if I feel under pressure to agree to something I am unsure about or don't want to do. I can identify who can help me if something happens online without my consent. I can explain how it may make others feel if I do not ask their permission or ignore their</p>
----------------------	--	---	---	---	---

		<p>experiencing bullying.</p> <p><b>EFCW: Self-Image and Identity</b></p> <p>I can explain how other people may look and act differently online and offline</p> <p>I can give examples of issues online that might make someone feel sad, worried, uncomfortable or frightened.</p> <p>I can give examples of how they might get help.</p>		<p>homes connected to the internet and give examples (e.g., lights, fridges, toys, televisions).</p>	<p>answers before sharing something about them online.</p> <p>I can explain why I should always ask a trusted adult before clicking 'y's', 'agree' or 'accept' online.</p>	
<b>Assemblies/ Theme days</b>	<b>Autumn 1</b>	<b>Autumn 2</b>	<b>Spring 1</b>	<b>Spring 2</b>	<b>Summer 1</b>	<b>Summer 2</b>
	<p><b>Project Evolve - Health, well-being, and Lifestyle</b></p> <p>I can explain rules to keep myself safe when using technology both in and beyond the home.</p>	<p><b>EFCW - Online Reputation</b></p> <p>I can recognise that information can stay online and could be copied.</p> <p>I can describe what information I should not put online without asking a trusted adult first.</p>	<p><b>Anti-Bullying Week</b>– November.</p> <p><b>EFCW - Online Bullying:</b></p> <p><b>Safer Internet Day</b></p> <p>Staying safe online</p> <p>Assembly – (Project Evolve) – Importance of not using devices before bedtime.</p>	<b>EFCW - Privacy and Security</b>	<b>EFCW - Managing Online Information</b>	<b>EFCW - Online Relationships</b>

<b>Key vocabulary</b>	<b>EYFS</b> Internet Online Safe Healthy Trusted Information	<b>Year 1</b> Permission Password Personal information Protect Rules Online llying	<b>Year 2</b> Private Accounts Consent Content Report
<b>Cultural capital</b>	Understand that there are different technologies and devices which serve multiple purposes.	Understand that when using technology, rules need to be followed.	Understand that some information is private and not to be shared.
<b>Sticky knowledge</b>	To recognise kind and unkind behaviour.	To be able to identify the positives and negatives when using technology. To understand how your online activity can affect others.	To know the risks of sharing information without permission. To understand the type of information you should/should not share online.