

# Polesden Lacey Infant School



## Online Safety Policy

Status	Statutory
Review Cycle	Every Three Years
Date written/last review	January 2021
Date of next review	January 2024
Online Safety Coordinator	Laura Mathews

Signed Headteacher

Date

**This policy has been reviewed in line with the updated Keeping Children Safe in Education.**

---

## 1. Context:

At Polesden Lacey Infant School online safety is an integral part of our safeguarding culture. As such we ensure that all staff members are trained in knowing how to recognise online safeguarding issues and the procedures to follow should an issue arise as well as teaching children what they should do if they have any concerns when using the internet.

The staff and governors of Polesden Lacey Infant School recognise they have a duty to ensure that all pupils are able to make a valuable contribution to society and this is only possible to achieve if we ensure that pupils develop and apply their computing capability effectively in their everyday lives.

The school is aware of its responsibilities in ensuring that ICT usage by all network users is responsible, safe and secure. There are relevant and comprehensive policies in place which are understood and adhered to by network users.

It is the duty of the school to ensure that every child in their care is safe, and the same principles apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements of school policy.

## 2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive online safety education programme for pupils, staff and parents.

## 3. Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of governing body, aims to embed safe practices into the culture of the school.

Designated Safeguarding Lead Details of the school's Designated Safeguarding Lead (DSL) and Deputy DSLs are set out in our Safeguarding and Child Protection Policy.

The DSL in conjunction with the online safety coordinator, takes lead responsibility for online safety in school, in particular:

- In ensuring that staff understand this policy, and that it is being implemented consistently across the school.
- Working with, ICT support (Click on It) and other staff, as necessary to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged (see appendix G) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour Policy.
- Updating and organising/delivering staff training on online safety (appendix F is the online safety audit with use with staff to identify online safety training needs.)
- Liaising with outside agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Governing Body.

The DSL should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from the four areas of risk as categorized by the DFE in KCSIE\* 2021:

- **Content;** being exposed to illegal, inappropriate or harmful content, for example; pornography, fake news, racism, misogyny, self harm/suicide, anti-semitism, radicalisation and extremism.
-

- **Contact:** being subjected to harmful online interaction with other users for example peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood or causes, harm, for example making, sending and receiving explicit images (consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and or financial scams. This also includes:
  - Sharing of personal data.
  - Access to illegal / inappropriate materials.
  - Inappropriate on-line contact with adults / strangers.
  - Potential or actual incidents of grooming.
  - Online-bullying.
  - Monitoring incident logs.
  - Consulting stakeholders – including parents / carers and the students / pupils about the online safety provision.

The Headteacher ensures that the policy is implemented and compliance with the policy monitored.

Our online safety Coordinator, ensures they keep up to date with online safety issues and guidance through liaison with the Local Authority and through organisations such as Child Exploitation and Online Protection (CEOP), INEQE Safeguarding Group and National Online Safety. The school's online safety coordinator ensures the Headteacher, senior leadership and Governors are updated as necessary.

Governors have an overview understanding of online safety issues and strategies at this school. The online safety coordinator will update the governing body at least once a year to ensure that governors are aware of changes in local and national guidance.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school online safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' online safety policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social networking;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- E-Bullying / Cyberbullying procedures;
- Their role in providing online safety education for pupils;
- Their role in providing relationships education with specific reference to the use of social media.

All staff are required to sign the school's Acceptable Use policy (see appendix C). The signed copies are kept in the individual member of staff's file and a copy is given to them as an aide memoire.

Staff are reminded / updated about online safety matters at least once a year.

---

The school includes online safety in our curriculum and we ensure that every pupil has been educated about safe and responsible use. (Please see Appendix D and E). The children have written E Safety Rules which are used throughout the year and displayed in all classrooms. (Please see Appendix F)

Pupils need to know how to control and minimise online risks and how to report a problem.

Visitors, Volunteers and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to follow it. If appropriate, they will be expected to agree to the terms of acceptable use.

The school engages with parents in relation to Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The school will take every opportunity to help Parents understand these issues through Parents' Evenings, newsletters, letters, the Polesden Lacey Infant School website and information about national / local online safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to Parents' sections of the website and on-line pupil assessment systems i.e. Tapestry.
- Their children's personal devices in the school.

Parents can seek further advice on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-andcarers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <https://www.childnet.com/parents-and-carers>
- Parent Information on Online Sexual Harassment: <https://www.childnet.com/resources/online-sexual-bullyingadvice-for-parents-and-carers-of-9-12-year-olds>

Parents can report any concerns they have regarding anything which has happened outside school via CEOP: <https://www.ceop.police.uk/Safety-Centre/>

The school uses the weekly newsletter to highlight online safety updates or news concerns to parents. There are also online safety workshops held bi-annually for parents to attend.

#### **4. Communications**

It is important that all staff feel confident to use new technologies in teaching. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies. Staff understand the rules for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding. ICT use is widespread and Induction of new staff includes a discussion of the school's online safety policy.

- Staff are aware that Internet traffic is monitored and can be traced to the individual user.
-

- Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use are supervised by senior leaders and have clear procedures for reporting issues. Staff training in safe and responsible Internet use and on the school online safety Policy is provided as required.

### **How will parents' support be enlisted?**

Internet use in pupils' homes is an everyday activity. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school is able to help parents plan appropriate supervised use of the Internet at home.

- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents is encouraged including; parent evenings with demonstrations and suggestions for safe home Internet use
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents - this can be found on the school's website.

## **Cyber-Bullying**

### **Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy and Anti-bullying policy.)

Children can abuse each other (sometimes referred to as Peer-on-Peer Abuse) and this can take the form of cyber-bullying, this can have a lasting emotional impact on a child/ren.

### **Preventing Online/Cyber-Bullying at Polesden Lacey Infant School**

We take any form of bullying very seriously and will take swift action to deal with any such incidents. The Headteacher/DSL will investigate the report of any online bullying and will take appropriate action as set out in our Behaviour and Anti-Bullying Policies. To help prevent cyber-bullying, we will ensure that pupils understand what cyber-bullying is (in an age appropriate way) and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school offers a comprehensive package of information to parents and carers to support them in knowing how to keep their children safe online. This includes regular information such as support in setting up parental controls on electronic devices, parent Online Safety Meetings with a specialist Online Safety Advisor.

### **Dealing with Alleged Incidents of Cyber-Bullying**

In relation to a specific incident of cyber-bullying, the school will follow the procedures as set out in our Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. (Please see Appendix A for flow chart) 9 The DSL will consider whether the incident should be reported to the Police if it involves illegal material, and will work with external services if it is deemed necessary to do so. Parents will be informed and asked to attend a meeting at school with the Headteacher/DSL.

## **How will complaints regarding online safety be handled?**

The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device.

Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions.

Sanctions available include:

- interview/counselling by online safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system];
- referral to LA / Police.

Our online safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. The Headteacher will follow the Online Safety Escalation Protocol (see appendix A).

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to child protection are dealt with in accordance with school / LA child protection procedures. (see appendix A)

## **6. Managing the Internet Safely**

### **The risks**

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be considered inappropriate and restricted elsewhere. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of and respond responsibly to any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

### **Technical and Infrastructure: Awaiting info from RM safety net.**

This school:

- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
  - Never allows pupils access to Internet logs;
  - Never sends personal data over the Internet unless it is encrypted or otherwise secured;
-

- Uses 'safer' search engines with pupils where appropriate

### **Policy and Procedures:**

This school:

- Supervises pupils' use at all times, as far is reasonable.
- We use the RM Safety Net filtering system which blocks sites that fall into categories such as pornography, race hatred, radicalisation, child sexual exploitation, gaming, sites of an illegal nature;
- Staff preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments.
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs users that Internet use is monitored;
- Informs staff and pupils that they must report any failure of the filtering systems directly to the computing leader.
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures the named child protection officer has appropriate training;
- Makes information on reporting offensive materials, abuse / bullying etc. available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police/LA.
- Adheres to our Safeguarding policy when a child makes a disclosure (See Appendix 2)

### **Education and training:**

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or Technician.
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report abuse;
- Has a clear, progressive online safety education programme. – We currently use Natterhub.

Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
  - to talk to an adult if they see something that has upset them
  - to understand information online may not be factual
  - the importance of keeping personal information private
  - to carefully explore why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
  - to know not to use new websites or games without permission from parents;
-

## **6. Copyright and Plagiarism**

This school;

- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on- line gaming / gambling;
- ensures staff know how to encrypt data where the sensitivity requires and that they understand data protection and general ICT security issues linked to their role and responsibilities;
- makes training available to staff on the e-safety education program;
- runs a rolling programme of advice, guidance and training for parents, including:
- information in school newsletters; on the school web site and/or MLE;
- demonstrations, practical sessions held at school;

## **7. Password policy**

- This school makes it clear that staff must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords and email passwords are changed at least twice a year.
- The children use a class log in and password when using the laptops.

## **8. Managing e-mail**

E-mail is now an essential means of communication for staff in our schools and increasingly for pupils and homes.

This school:

- does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for any communication with the wider public
- Contacts the police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law
- Manages accounts effectively, with up to date account details of users
- Reports messages relating to or in support of illegal activities.
- Staff use Microsoft 365 e-mail systems for professional purposes;

## **9. Use of Digital and Video images**

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
  - Uploading of information is restricted to the website team.
  - The school web site complies with the school's statutory requirements
-



- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities is not published;
- Photographs published on the web site do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted periodically - unless an item is specifically kept for a key school publication;
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website.
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are taught about how images can be abused in their online safety education programme;

## **10. Managing equipment**

The computer system / network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

***The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.***

To ensure the network is used safely this school:

- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
  - Makes clear that pupils should never be allowed to log-on or use teacher and staff logins - these have far less security restrictions and inappropriate use could damage files or the network;
  - Makes it clear that no one should log on as another user - if two people log on at the same time this may corrupt personal files and profiles;
  - Has set-up the network with a shared work area for staff. Staff are shown how to save work and access work from these areas;
  - Requires all users to always log off when they have finished working or are leaving the computer unattended;
  - Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
  - Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  - Maintains equipment to ensure Health and Safety is followed;
  - Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
  - Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
  - Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
  - Reviews the school ICT systems regularly with regard to security.
-

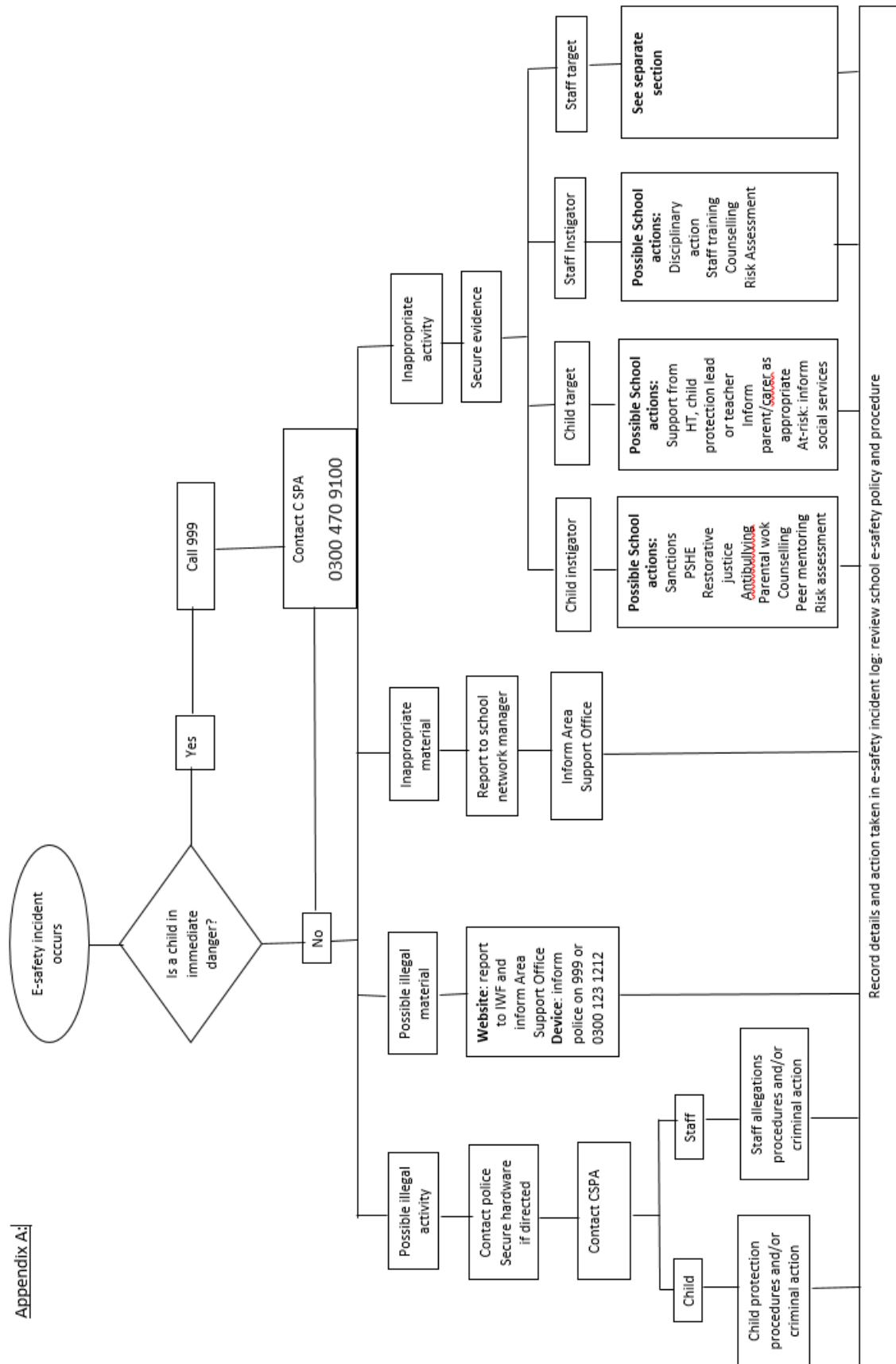
## **11. Personal mobile phones and mobile devices**

- Mobile phones brought into school are entirely at the staff member or parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff members may use their phones during school break times.  
All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. toilets.

### ***Students' use of personal devices***

- We do not allow pupils to bring electronic devices into school e.g. tablets, phones, smart watches or iPads
  - When using their own devices at home children are expected to behave in the same way that they do in school and follow our E-safety rules.
  - Parents are supported in keeping their children safe online via a termly newsletter and guidance is given to put parental controls in place on all their online devices
  - During remote online learning sessions parents are expected to be present.
  - Parents are required to give permission or their child/children to take part in Zoom meetings (Appendix E)
-

## Appendix A:



## Appendix B:

# HANDLING A DISCLOSURE

- Don't promise to keep it to yourself
- Reassure but do not question them further
- Don't tell them that they have done nothing wrong or that they have done well
- Don't use any form of language that could be deemed as rewarding

## **Appendix C:**

### **STAFF, GOVERNOR AND VISITOR**

#### **ACCEPTABLE USE POLICY (This should be read in conjunction with our Staff Code of Conduct)**

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Laura Mathews school's online safety coordinator.

- I will only use the school's email/Internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data and sensitive information (such as data held on SIMS, memory sticks or on laptops) is kept encrypted and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without the permission of Laura Mathews or computing technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not use my mobile phone in sight of children and will respect my colleagues when using it in the staffroom.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headteacher.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not use personal devices to take images or film of children at school.

#### **User Signature**

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature..... Date.....

---

## Polesden Lacey Infant School – Computing Curriculum Map 2019-2020

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
<b>EYFS</b>	<p><b>E-Safety</b></p> <p>To learn how to use the mouse pad on the laptops.</p> <p>To use click and drag in order to complete a simple program / print a picture.</p> <p>To know how to use the digital camera / <u>ipad</u>.</p> <p>To know how to operate remote control cars / programmable toys (<u>codapillar</u>).</p>	<p><b>E-Safety</b></p> <p>Identify lights and classroom equipment that use electricity.</p> <p>To learn that electricity is dangerous.</p> <p>To know that a battery is a portable supply of electricity.</p>	<p><b>E-Safety</b></p> <p>Use 2paint to create a picture.</p> <p><b>Safer Internet Day</b></p>	<p><b>E-Safety</b></p> <p>Use the computer keyboard to write names.</p> <p>To take photos using the digital camera and comment on the finished result.</p>	<p><b>E-Safety</b></p> <p>Use technology for different purposes.</p> <p>To use a digital microscope for investigating mini beasts.</p>	<p><b>E-Safety</b></p> <p>Operate remote control car to move forward, change direction and adjust speed.</p>
<b>Year 1</b>	<p><b>E-Safety</b></p> <p>Instructions (Simon says).</p> <p>Sequencing &amp; Ordering (make a sandwich).</p> <p>Google –Earth (UK).</p> <p>2paint –<u>Kandinsky</u> (art) Open the program/ save w/ support.</p> <p><b>TECHNOLOGY WEEK</b></p>	<p><b>E-Safety</b></p> <p>Turning Laptops on and off.</p> <p>2 type, capital letters, save &amp; print – thank you letters to PL.</p> <p>Instructions and programming -Lego.</p> <p>Recording dance routines.</p>	<p><b>E-Safety</b></p> <p>Bee – Bots programming algorithm &amp; debugging.</p> <p>2paint – Firework art save and print.</p> <p><b>Safer Internet Day</b></p>	<p><b>E-Safety</b></p> <p>2 paint – Castle in the Sun. Open programme/ save/ print.</p> <p>Espresso Coding 1a.</p> <p>Pictogram – hours of sunlight (supported).</p>	<p><b>E-Safety</b></p> <p>Espresso Coding 1b.</p> <p>Creating own code/app, save and share.</p>	<p><b>E-Safety</b></p> <p>Research – Amazon.</p> <p>Google Earth – Amazon.</p> <p>Scratch Junior Introduction.</p>

Year 2	E-Safety	E-Safety	E-Safety	E-Safety	E-Safety	E-Safety
	<p>Log on, off.</p> <p>Word- enter, delete, caps lock button font- colour, size.</p> <p>2 paint- superhero pictures, tiling (Andy Warhol?).</p> <p>Technology week- Lego programming, bee bots.</p>	<p>Espresso Coding – Unit 2a.</p> <p>Research –fire of London, Museum of London websit.</p> <p>Word- Christmas poem font- colour, style, size spell check.</p>	<p>Google Maps- local area, navigating along a street, comparing Isle of Struary with Bookham.</p> <p>Research- Isle of Struary.</p> <p>Bar chart- Bird watching day.</p> <p>Safer Internet Day</p>	<p>Data handling- different types of graphs, representations.</p> <p>Beebots- position and direction, programming.</p> <p>Making repeating patterns.</p> <p>Charanga- composing.</p>	<p>2 paint- gruffalo pictures, reflective symmetry (butterfly).</p> <p>Badger watch- camera.</p> <p>Research- wildlife.</p> <p>Charanga- composing.</p>	<p>Espresso Coding- Unit 2b.</p> <p>creating own code/app. Save and share.</p>

Appendix E -

Progression of Skills for Online Safety			
	EYFS	Year 1	Year 2
E-Safety and E-Sense	<p>Talk about good and bad choices in real life e.g. taking turns, saying kind things, helping others, telling an adult if something upsets you.</p> <p>Talk about good and bad choices when using websites – being kind, telling a grown up if something upsets us &amp; keeping ourselves safe by keeping information private</p>	<p>Think about why it is important to have a password.</p> <p>Explain what personal information is.</p> <p>Know how to tell an adult when something unexpected or worrying is seen online.</p> <p>Explain why it's important to be kind and polite.</p> <p>Recognise an age appropriate website.</p> <p>Agree and follow sensible e-safety rules.</p>	<p>Explain why it is important to keep passwords and personal information private.</p> <p>Know when to talk to an adult about things I see online.</p> <p>Explain why children should go online for a short amount of time.</p> <p>Explain why it is important to be kind and polite online and in real life.</p> <p>Understand that not everyone is who they say they are on the internet.</p> <p>Agree and follow sensible e-safety rules, explaining why they are important.</p>

**Polesden Lacey Infant School**

**E Safety Rules January 2020**

I will tell an adult when I am using technology: e.g. tablet, iPad, phone or computer.

I will ask an adult before playing a new game or downloading a new app.

I will only play games that are suitable for my age.

I will only click on things that I understand.

I will ask for help if I see something I do not like.

I will keep my personal information private.

I will spend a sensible amount of time on technology at home.

I will treat others as I want to be treated by using kind words.

---



## Zoom permission

In order to maintain contact with the staff and pupils during the COVID-19 closure we will be using Zoom to share story telling sessions and a daily online session with the children. This is enabling the children to see and hear their teachers and see each other. We feel that the impact is hugely beneficial. As always the safety of our pupils and staff is off the highest importance and with this in mind we have put some protocols in place. Please could you complete this form giving your permission for you and your child to take part in Zoom sessions.

\* Required

Child's name \*

Your answer

I agree for my child to join the online teaching session and watch the story telling sessions that Polesden Lacey Infant School will stream using Zoom. \*

Agree  
Disagree

A parent or carer will always be present during the Zoom sessions. \*

Agree  
Disagree

I understand that the teacher hosting will record the Zoom sessions. This will not be shared but kept for up to 1 year as a record of the session. \*

Yes  
No

I will not record or screen shot any of the sessions. \*

---

Agree  
Disagree

The school will email the invites to the parent. I will not share these invites with anyone else. \*

Agree  
Disagree

When in the Zoom sessions we will continue to follow the Polesden Lacey Infant School Behaviour code and be respectful to others in the session. \*

Agree  
Disagree

---