

# Denmead Infant School

## E-safety Policy

| Our Denmead Infant Curriculum Aims    | Happy together<br>Secure relationships and exemplary pastoral care                                                 |                                                                                                   | Growing together<br>Irresistible learning environments where adults and children thrive on challenge                              |                                                                                                  | Aiming high<br>Achieving excellence for all                                                                                     |                                                                                                |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Values to ensure a learning adventure | Resilience<br>                    | Independence<br> | Courage<br>                                      | Creativity<br> | Collaboration<br>                            | Respect<br> |
| Our vision for all of our children    | We are empowering our children to be confident individuals who are able to lead safe, healthy and fulfilling lives |                                                                                                   | We want our children to grow into responsible citizens who make a positive contribution to local, national and global communities |                                                                                                  | We enable our children to develop skills, knowledge, understanding and enjoyment that sustain a lifetime of successful learning |                                                                                                |

Today's children are growing up in an increasingly complex world, living their lives seamlessly off and online. The internet, and devices that utilise it, are embedded in everyday life for the majority of people and provide a powerful and useful tool for children's learning. Use of the internet is also part of the Computing National Curriculum.

At Denmead Infant School, staff and other adults show vigilance and care in ensuring children are **happy** and safe online. As new technologies are developed and improved children and staff alike can **grow** their knowledge and understanding whilst exploring a variety of digital technologies. They will **aim high** through exploration and teacher modelling of these technologies to ensure **every day is a learning adventure**.

### Aims

All children will have the opportunity to:

- learn to use the internet and other digital technologies safely and responsibly
- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies
- develop a positive attitude to the internet and develop their ICT capability and confidence through both independent and collaborative working
- learn how to use the internet safely and how to act if they come across something inappropriate

### Pupil's use of the internet

All children will:

- use the internet to enhance their learning experience
- have opportunities to engage in independent and collaborative learning using the internet and other digital technologies
- be taught how to effectively use the internet for research purposes
- be taught to evaluate information on the internet
- be taught how to report inappropriate web content

### Roles and Responsibilities of adults

Approved: February 2025

Next Review: February 2027

All staff, volunteers, governors and other adults working at the school must model appropriate behaviour in relation to use of the internet, and must read the Acceptable Use of ICT policy before using any information communications technology on site.

### **Headteacher**

The Headteacher:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- liaises with the Local Authority
- liaises with school technical staff
- ensure that developments at Local Authority level are communicated to the Digital Leader
- ensure that the Governing Body is informed of e-safety issues and policies.
- make all staff aware that internet traffic can be monitored and traced to the individual user, and that safe, professional conduct is essential
- assume editorial responsibility for all content on the school website, Facebook page, ensuring that it is accurate, appropriate and accessible
- report any material believed to be illegal to appropriate agencies such as the Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).

### **Designated Safeguarding Leads**

The designated safeguarding lead is trained in e-safety issues in order to respond to child protection / safeguarding issues arising from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- reports of internet misuse by staff, parents/carers or children

### **All school staff**

All school staff must ensure that:

- they have an up to date awareness of e-safety matters and the current school e-safety policy and practices
- e-safety issues are embedded in all aspects of the curriculum and other activities
- children are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- children are supervised when using the internet
- they take every necessary action to protect the security of all confidential data. This includes children's names, photos and assessment information in line with the school's Data Protection Policy
- they report any suspected misuse or problem to the head teacher for investigation
- all digital communications with children and their parents / carers are on a professional level

**All staff must ensure that they have read and understood their responsibilities within the following documents.** (These are all contained within the Hampshire Manual of Personnel Practice).

- Staff Acceptable use of IT
- School Social media Policy
- Dos and Don'ts (use of IT) – advice to staff
- Dos and Don'ts (cyberbullying) - advice to staff

They are also reminded that:

- Staff should exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children
- Staff should make appropriate use of the security settings available
- Inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal
- Under no circumstances should any school staff have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites
- School staff are advised not to accept friendships via their social networking with parents, ex-parents and governors. Where staff do accept such friendships, they must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts
- School staff are fully entitled to accept friendships with colleagues via their social networking site but should take care in communications exchanged in areas of public access
- Senior staff and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues as contacts on social networking sites
- Staff must share any concerns that may arise on social media with the head teacher

### **Computing Lead**

The Computing Lead will:

- provide guidance and resources to support other staff's use of the internet and digital technologies / devices
- provide support for parents/carers through newsletters, meetings
- liaise with IT support company ensuring effective filtering is set and monitored

### **Parents / Carers**

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will help parents understand these issues through parents' evenings, newsletters, letters, website and information about national e-safety campaigns.

Parents / carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Should the school be concerned that a child has access to websites or games that are not appropriate for their age, or has access to a social media platform then they will contact parents and carers as this may raise safeguarding concerns.

### **Governors**

The Governing Body will:

- be responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy and should be aware of how the internet is used in school through their regular monitoring visits.
- appoint a Digital Link Governor who will ensure that E-Safety is included as part of the regular review of child protection and health and safety policies
- support the Headteacher and/or designated E-Safety Leader in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment
- ensure that appropriate funding is authorised for e-safety solutions, training and other activities

### **Technical staff**

The school's IT technical support is provided by Drift IT

Our Technical Staff are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack

Approved: February 2025

Next Review: February 2027

- the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- they manage the filtering systems via a cloud portal as instructed by the school
- they respond to any reports made by school staff of inappropriate sites

### **E-safety Education**

E-safety should be an integral part of all aspects of school life and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum will be provided as part of Computing and PHSE curriculum. This will be regularly reviewed in order to ensure that it remains relevant and up to date
- Children will be taught how to adopt safe and responsible use both within and outside school
- Staff are expected to act as good role models in their use of digital technologies, the internet and mobile devices
- Children will be guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites they visit.

Materials provided by the following organisations will be used to teach children how to stay safe on-line:

- [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) – provided by CEOP the Child Exploitation and Online Protection Service
- [www.childnet.com](http://www.childnet.com) – which is linked to the UK safer internet centre
- [www.nspcc.org.uk](http://www.nspcc.org.uk) – who also provide online safety advice for parents

### **Use of digital and video images**

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment and saved on the open 'staffshare' area of the school network. The personal equipment of staff should not be used for such purposes.
- Photographs published on the website, or elsewhere that include images of children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's names will not be used anywhere on a website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school website, within newsletters or other places such as the local paper.

### **Communications**

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff must ensure that all communications related to their professional roles should be conducted using their school email accounts.
- Users must immediately report, to the nominated person the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on school systems i.e. Scopay, Seesaw, school email accounts. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Risks

Risk can be categorised into 4 main areas:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, 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 to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (<https://apwg.org/>). E-Safety Policy Autumn 2021 Page 4 of 8

## Email

- Pupils will only use approved school email addresses in school.
- Pupils will inform a member of staff if they receive inappropriate or abusive emails.

## Publishing web content

- The contact details on the school website should be the school address, admin office email address and telephone number.
- The website should respect and reflect property rights and copyright.
- Images of pupils should be selected carefully and be published only with the consent of the parents/carers and be presented in a way that reduces the opportunities for it to be reused elsewhere.
- Pupils' work can only be published on the school website if the parents have given specific and informed consent.

## Managing social media

- The school has a Social Media Policy (Add link to policy on website) which should be read in conjunction with this policy.

## E-Safety Complaints

- Instances of pupil internet or Learning Platform misuse should be reported to a member of staff.

Approved: February 2025

Next Review: February 2027

- Staff must log incidents reported to them and if necessary refer the matter to a senior member of staff.
- Instances of staff internet or other ICT misuse should be reported to, and will be dealt with by, the Headteacher.

### **Related policies**

This policy should be read in conjunction with the school's ICT Acceptable Use Agreement, Behaviour policy, Child Protection Policy and Confidentiality Policy. Any complaints relating to E-safety will be managed according to the school's Complaints Policy.

### **E-Safety in Classrooms**

Every classroom will display an E-Safety poster which children can refer to and help guide them if they find themselves in situations where they feel concerned. Whenever the internet is used to support learning in class, teachers will remind children how this is achieved safely.

### **Gaming**

Online gaming is an activity in which the majority of children and many adults get involved.

The school will raise awareness:

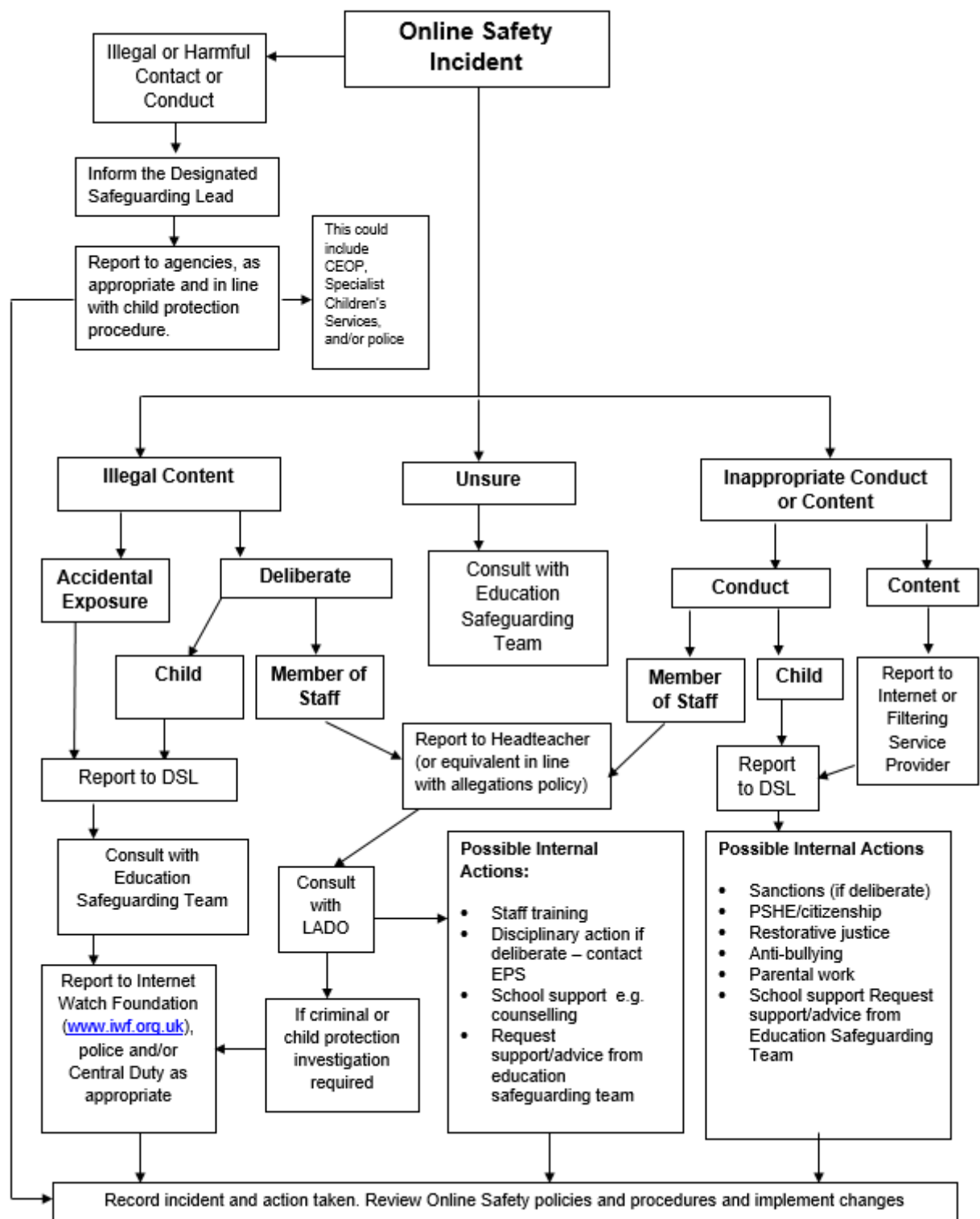
- By talking to parents and carers about the games their children play and help them identify whether they are appropriate
- By directing parents to materials to help them identifying the most effective way to safeguard their children by using parental controls and child safety mode
- By talking to parents about setting boundaries and time limits when games are played
- By highlighting relevant resources.

### **Managing emerging technologies**

New IT applications, both hardware and software, will initially be explored by the Digital Leader. Advice will then be put to the Leadership Team, enabling them to assess the educational benefits and potential risks. Training the school will ensure that all teaching staff (teachers and learning support assistants) have a basic understanding of E-Safety. Formal training will be provided for key staff. Ongoing dialogue will support an open culture where potential issues are identified, discussed and solutions agreed.

## **Appendix:                      Responding to an on-line safety concern**

If there is any suspicion that a website has been accessed which contains child abuse images, or if there is any other suspected illegal activity, the school will refer to the flowchart below for responding to online incidents and report immediately to the police.



# Being Safe on the Internet

When I use an iPad or Laptop I must remember to:-

