Ashdon Primary School

Online Safety Policy

Date adopted by Governing Body: **October 2021** Next Review: **October 2024**

SAFEGUARDING STATEMENT

Ashdon Primary School takes seriously the responsibility to protect the welfare of the children in its care, believing that "The welfare of the child is paramount" Children Act 1989.
This policy plays an integral part in our aim to safeguard the children and ensure their wellbeing in order to promote optimum development.

Aims

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'Online Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or pupil, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Roles and Responsibilities of the School

Governors/ Headteacher

It is the overall responsibility of the Headteacher with the Governing Body to ensure that there is an overview of Online Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Headteacher has designated an Online Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take responsibility for ensuring Online Safety is addressed in order to establish a safe IT learning environment. All staff and pupils are aware of undertakes this role within the school.
- Time and resources should be provided for the Online Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting Online Safety across the curriculum and has an awareness of how this is being developed, linked with the School Development Plan.
- The governor with responsibility for Safeguarding, ought to challenge the school/education setting or other establishment about having an Online Safety Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using IT, including:

Challenging the school about having:

  - Firewalls.
  - Anti-virus and anti-spyware software.
  - Filters.
  - Using an accredited ISP (Internet Service Provider).
  - Awareness of wireless technology issues.
  - A clear policy on using personal devices.

- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

Online Safety Lead

It is the role of the designated Online Safety Lead (which could also be the Computing, RSHE or Designated Safeguarding Lead already in role, but should be a senior member of the school and not a network manager) to:

- Appreciate the importance of online safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe IT learning environment within the school.
- Ensure that the Online Safety Policy is reviewed at least every three years, or sooner if required, with up-to-date information and that training is available for all staff to teach Online Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-a-lone PC and staff/children' laptops or ensure the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the RSHE, safeguarding and Computing leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct Online Safety information can be taught or adhered to.
- Transparent monitoring of the Internet and online technologies. Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.
- Work alongside the Computing Lead, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

Staff or Adults

It is the responsibility of all adults within the school to:

- Ensure that they know who the Designated Safeguarding Lead (and their alternate) is within school, so that any misuse or incidents can be reported which involve a child.
- Where an allegation is made against a member of staff it should be reported immediately to the Headteacher or Chair of Governors (if the allegation is about the Headteacher).
- Be familiar with the Behaviour & Discipline Policy, Anti-bullying Policy, Harmful Sexual Behaviour and Peer-on-Peer Abuse Policy, so that, in the event of misuse or an allegation, the correct procedures can be followed immediately. Appendix 1 gives an overview of how to respond to Online Safety incidents.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the Online Safety Lead.
- Alert the Online Safety Lead of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. Children and young people should know what to do in the event of an incident.
- Be up-to-date with Online Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- To have read and signed to say the agree to the terms of the Staff Code of Conduct, which includes an ICT Acceptable Usage Policy.

- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998 or GDPR. Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the Online Safety Lead.
- Use anti-virus software and check for viruses on their work laptop, memory stick or when downloading files from the Internet on a regular basis, especially when not connected to the school's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.

Pupils

Pupils should be:

- Involved in the review of Acceptable Use Agreement through the School Council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the My Online Safety Agreement (Appendix 2).
- Taught to use the Internet in a safe and responsible manner through the Computing and RSHE curriculums.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

In the Event of Inappropriate Use by Pupils

In the event that a child **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or minimise the window so that an adult can take the appropriate action. *The computer must not be turned off until a screen capture has been taken and saved, together with the website address written down*. Staff should share this information with the Online Safety Lead and the Designated Safeguarding Lead.

Pupils deliberately misusing online technologies should also be addressed by the school using our Behaviour & Discipline Policy, and, where appropriate our Anti-Bullying and Harmful Sexual Behaviour Peer-on-Peer Abuse policies.

The Curriculum and Tools for Learning

Our school teaches children how to use the Internet safely and responsibly. They should also be taught, through Computing and/or RSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave Year 6*:*

- Internet literacy.
- Making good judgements about websites and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- File sharing and downloading illegal content.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

We also specifically the children about the dangers of sharing personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- School.
- Clubs attended, where and when.
- Age or DOB.
- Names of parents.
- Routes to and from school.
- Identifying information, e.g. I am number 8 in the school football team.

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'.

Pupils with Additional Learning Needs

The school should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a pupil has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of online safety awareness sessions and Internet access.

School Website

The uploading of images to the school website should be subject to the same acceptable agreement as uploading to any personal online space. Permission is to be sought from the parent/carer prior to the uploading of any images.

External Websites

In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, school are encouraged to report incidents to the Headteacher and unions.

E-mail Use

Staff and governors will use their school-issued email addresses for any communication between school, other educational establishments and parents/carers home email address only. A breach of this may be considered a misuse.

The school currently does not issue pupils with individual email addresses.

Personal Mobile Devices

Staff are be allowed to bring in personal mobile phones or devices for their own use, but must not use personal numbers to contact children and young people under any circumstances.

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Before using a personal device within school lessons, authorisation should be sought from the Headteacher.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

Pupils are not allowed to use mobile devices in school. If a pupil is discovered with a device, then this will be kept in the school office for the remainder of the school day and the parents notified.

School-Issued Mobile Devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop or mobile phone, only this equipment should be used to conduct school business outside of the school environment.

Video and Photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school, there is access to devices that can take and/or view images and videos and stream live video.

Staff mobile phones, or personal photographic equipment/computer devices, should not be used to take images or videos of pupils.

The sharing of photographs via websites, or by any other means online, should only occur after permission has been given by the parent/carer and/or the members of staff who are featured in the photographs.

Any photographs or video clips uploaded should not have the name of a child displayed and/or as part of the filename.

Photographs should not be of any compromising positions or in inappropriate clothing, e.g. in a swimming costume.

It is current practice by external media, such as local and national newspapers, to include the names of children and young people in their publications. Photographs of children/young people should only be used in the media after permission has been given by a parent/carer.

Video-Conferencing and Webcams

Taking images via a webcam should follow the same procedures as taking images with a digital or video camera.

Permission should be sought from parents and carers if their child is engaged in video conferencing with individuals or groups outside of the school. This process should always be supervised by a member of staff.

Children need to tell an adult immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Agreement).

Managing Social Networking

The school prohibits the pupils using social networking sites, e.g. Facebook and Twitter, on school devices, or having their own devices on which to use these services during school hours.

Social Networking Advice for Staff

Social networking outside of work hours, on non-school-issue equipment, is the personal choice of all school staff. School equipment, including teacher laptops and the school mobile phone, should not be used with social networks. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent pupils from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with pupils outside of Headteacher authorised systems (e.g. school email account for homework or online learning purposes).
- Staff should ensure that full privacy settings are in place to prevent pupils from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by pupils).

Filtering and Other Online Protection.

The broadband connectivity has a filter system which will be set at an age-appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.

Anti-virus and anti-spyware software are used on all network and stand-alone PCs or laptops and is updated on a regular basis.

A firewall ensures information about children and young people and the school cannot be accessed by unauthorised users.

Monitoring

The Online Safety Lead should be monitoring the use of online technologies by children and young people and staff, on a regular basis.

Teachers should monitor the use of the Internet during lessons and also monitor the use of e-mails from school on a regular basis.

Links to Other Policies – Behaviour & Discipline and Anti-Bullying Policies

Please refer to the Behaviour & Discipline Policy/Anti-bullying Policy for the procedures in dealing with any potential bullying incidents via any online communication, such as mobile phones, e-mail or blogs.

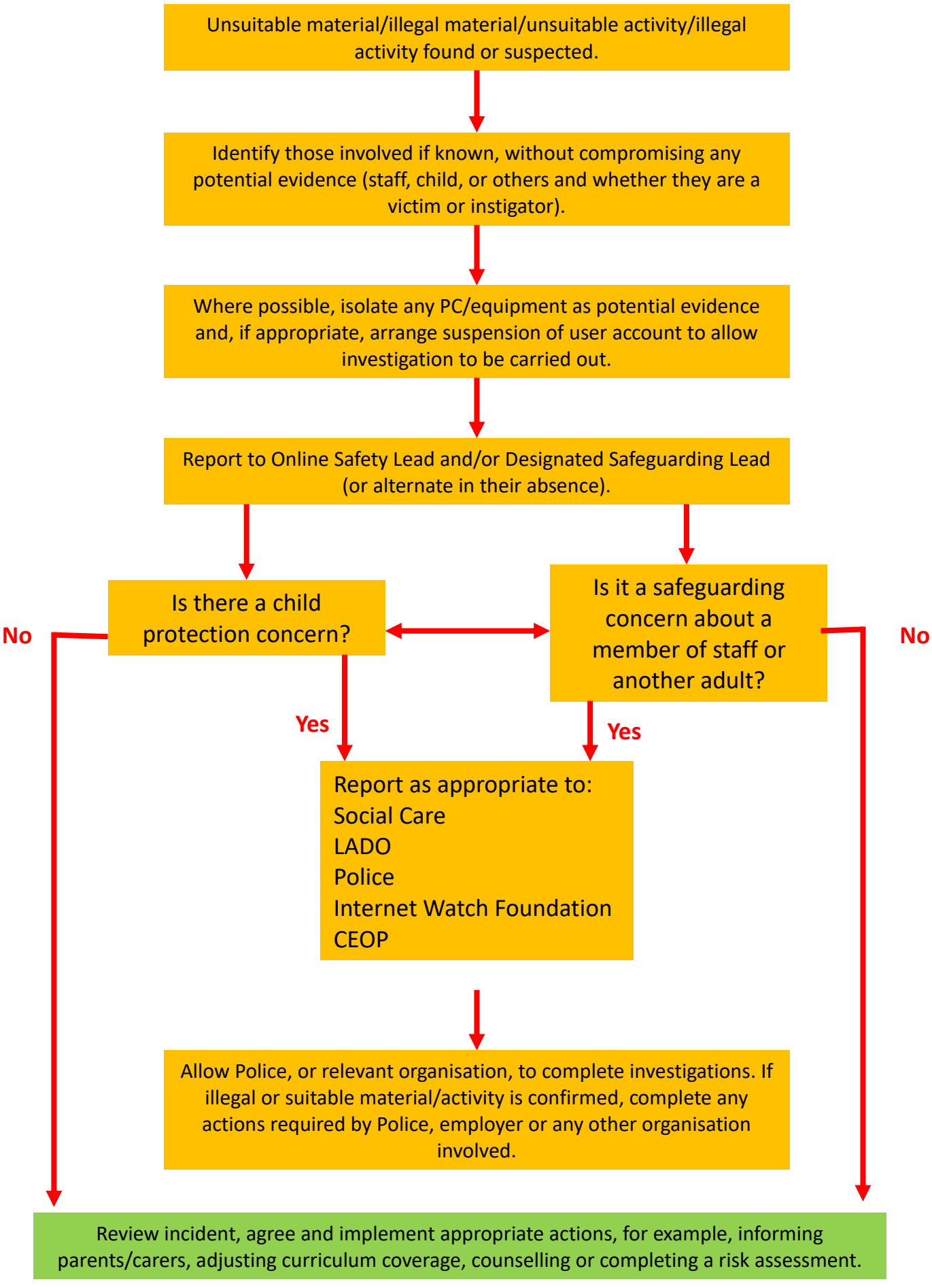
All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all Computing and RSHE materials for children and young people and their parents/carers. People should not treat online behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

Health and Safety

Refer to the Health and Safety Policy and procedures of the school and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

Appendix 1:

Online Safety Incident Flowchart



Appendix 2:

My Online Safety Agreement – Children

This is my agreement for using the Internet safely and sensibly at school.

- I will only go online in school, when a member of staff is with me.
- I will learn how to use the Internet safely and sensibly.
- I will be polite and friendly when talking or sending a message online.
- Staff will tell me who I can speak to online.
- I won't share my address, phone number, last name or passwords with people online.
- I will never put pictures or videos online unless allowed to.
- If I see anything on the Internet that makes me feel uncomfortable or upset, I will speak to an adult as soon as possible.