Wallace Fields Infant School and Nursery

Online Safety Policy

Wallace Fields Infant School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Reviewed: October 2023 **Next Review: September 2024**

Wallace Fields Infant School is proud to be a part of South Farnham Educational Trust.

Document ID/Name	E-Safety Policy
Date	November 2019
Document Location	P:\Policies\WFIS Master Policies\E-Safety Policy.docx
Version	4
Author	Christina Lane
Next Review Date	May 2022

Document History

Date	Version	Amended By	Comment (e.g. reason for version change)
16.11.15	1	Ceri Jewell	Tri Annual policy review
30.05.19	2	Christina Lane	Tri Annual Policy review
16.06.19		Nicky Mann	Ratify by SLT
03.10.19	3	Christina Lane	Amended E-Safety Incident section to reflect Anti-Bullying policy
30.03.20	4	Christina Lane	Amended to include Purple Mash
15.01.21	5	Anne-Marie Nicholson	Amended Section 11 to reflect use of emails at home during Covid Lockdown
15.09.22	6	Esme Holmes	Tri Annual policy review
17.10.23	7	Annabel Male	Updates to bring in line with Trust policy

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, mobile technology, social media, data handling and the use of images.

At Wallace Fields Infant School & Nursery we aim to:
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk
Our approach to online safety is based on addressing the following categories of risk:
- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Using this policy
This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:
- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Using this Policy
- The Online Safety Policy has been written based on best practice and government guidance. It has been agreed by Senior Management and approved by Governors.
- The Online Safety Policy was reviewed in Autumn 2023.
- The policy was approved by Trustees in September 2023.
- The Online Safety Policy and its implementation will be reviewed annually. The next review is due in Autumn 2024.
- The Online Safety Policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site.

This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.

• The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff or as a pupil.

Introduction

In line with current expectations the school has a computer system which gives the children access to the Internet.

Usually, the resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher.

The problems and issues that have been highlighted by the media concern all schools. Whilst some of the media interest is hype, there is genuine cause for concern that children might access unsuitable material accidentally.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet
- Describe how these fit into the wider context of our discipline and PSHCE policies
- Demonstrate the methods used to protect the children from sites containing pornography, racist or politically extreme views and violence.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents and guardians.

We feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

The online safety Policy is part of the School Improvement Plan and relates to other policies including those for Computing, bullying and for child protection.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between our systems and networks and the more open systems outside school.

• The school will use a recognised internet service provider or regional broadband consortium.

• The school will ensure that all internet access has age-appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.

• The school will ensure that its networks have virus and anti-spam protection.

• Access to school networks will be controlled by personal passwords.

• Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform future Online Safety policies.

• The security of our systems and networks will be reviewed regularly.

- All staff that manage filtering and monitoring systems will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

All staff's responsibilities for filtering and monitoring:

- Monitor what is on pupils' screens.
- Teach children about online safety using MTP.
- Know how to report safeguarding and technical concerns, if:
    - You witness or suspect unsuitable material has been accessed
    - You are able to access unsuitable material
    - You are teaching topics that could create unusual activity on the filtering logs
    - There is failure in the software or abuse of the system
    - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - You notice abbreviations or misspellings that allow access to restricted material

Governors' responsibilities for filtering and monitoring:

- Make sure the DSL takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role.
- Make sure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of their safeguarding training.
- Review the DfE's filtering and monitoring standards
- Identify and assign roles and responsibilities
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting T&L
- Have effective monitoring strategies in place that meet their needs
- Discuss with IT staff and service provider what needs to be done to support the school
- Assign a member of SLT and a Governor to be responsible for filtering and monitoring.

Parents'/Carers' responsibilities for filtering and monitoring:

- Engage with support and guidance provided by the school to ensure that home devices have appropriate levels of filtering and monitoring in place.
- Monitor their children's online activity, including mobile phone use, to ensure that they are behaving responsibly and appropriately online.
- Notify the school with any concerns or incidents relating to inappropriate activity online.

Wallace Fields Infant School & Nursery will provide an age-appropriate Online Safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety (including age restrictions, content and personal data).

Pupils will be taught about Online Safety as part of the curriculum based on the National Curriculum for Computing. It is also taken from the guidance on relationships education, relationships and sex education and health education (RSHE).

In Key Stage (KS) 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating Parents and Carers about Online Safety

We will endeavour to raise parents/carers' awareness of online safety in letters or other communications home. This policy will also be shared with parents/carers.

The school will inform parents/carers of:
- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or a DSL.

Protocols

Email
- Staff may only use approved email accounts on our systems and networks.
- Incoming email should be treated as suspicious and attachments should not be opened unless the author is known.
- Pupils will be given restricted email accounts in line with safeguarding procedures – this is purely for the purpose of logging into a Chromebook and learning to save to their Google Drive.

Published Content – e.g. School Website, school social media accounts
- The contact details will be the school address, email and telephone number. Staff and pupil's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work
- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in the Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media including the school learning platform
- The school has a separate social media policy.
- Staff and pupils should ensure that their online activity both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the community

Use of personal devices
- Personal equipment may be used by staff to access our systems and networks provided their use complies with the Online Safety Policy and the Acceptable Use Policy.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data
- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to school systems.

Policy Decisions

Authorising Access

• All staff (including teaching staff, teaching assistants, support staff, office staff, trainee teachers, work experience trainees, ICT technicians and governors) must read and sign the Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy before accessing our systems and networks.

• The school will maintain a current record of all staff and pupils who are granted access to our systems and networks.

At Key Stage1, access to the internet will be by adult demonstration with supervised access to specific, approved online material, which supports the learning outcomes planned for the pupils age and ability.

• People not employed by the school must read and sign an Acceptable Use of Computers, IT Equipment, Internet and Email (Visitors) Policy before being given access to the internet via school equipment.

• Parents/carers will be asked to sign and return a consent form (Acceptable Use of the School Computers) to allow use of technology by their child.

Assessing risks

• The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey County Council can accept liability of the material accessed or any consequences of internet access.

Handling Online Safety Complaints

• Complaints of internet misuse will be dealt with according to the school behaviour and relationships policy.

• Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

• Should any pupils encounter any offensive materials online accidentally they are expected to report it immediately to a teacher or teaching assistant, so that the Service Provider can block further access to the site.

• The Teacher or Teaching assistant should record the incident on the school's safeguarding system, CPOMS, which is then reviewed by the Designated Safeguarding Lead. Relevant parents will be informed. All incidents are monitored by a member of the Senior Leadership Team.

• The Head teacher and DSL should use the flow chart (Appendix 1) along with the screening tool and the Surrey Child Protection Procedures to determine next steps in supporting the child involved in the incident. Schools' DSL will be conversant with these and the processes for referral.

• Should any pupils encounter any cyber bullying by other pupils in the school, this should be recorded on CPOMS by the staff member to which the information was disclosed, in line with our Anti-Bullying Policy.

• The Designated Safeguarding Lead will inform the head teacher/deputy head of the incident recorded on CPOMS.

• The head teacher/deputy head teacher will interview all concerned and will add further action to CPOMS.

• Class teachers and support staff (as appropriate) will be kept informed.

• Parents will be kept informed.

• Appropriate disciplinary action will be taken.

• The log of online safety incidents will be monitored and reviewed regularly to ascertain whether any changes need to be made, e.g. to the school's policies, anti-bullying policies, AUPs, training, curriculum content.

Harms and Risks

Navigating the Internet and Managing Information

- Pupils will learn how to navigate the internet safely as part of their Computing lessons (details can be found in the Computing Policy).
- Due to the complex nature of the internet, pupils will be encouraged to consider information presented to them with caution, ensuring that they consider the reliability of the source.
- Topics will include considering age restrictions, disinformation/misinformation, fake websites and scam emails, online fraud and personal data (including protecting passwords and privacy settings)

Staying Safe Online

- Alongside the Computing curriculum content, pupils will learn how to stay safe online from outside agencies, including the Police and the NSPCC.
- Pupils will receive age specific advice covering the following topics:

O online abuse (e.g. sexual harassment, bullying, trolling and intimidation)
O online challenges and identifying whether they are safe or not
O content which incites
O fake profiles (i.e. adults posing as children or 'bots')
O grooming (e.g. radicalisation, Child Sexual Abuse and Exploitation and gangs)
O risks linked to live streaming
O interacting with known contacts to avoid unsafe communication

Wellbeing

- At Wallace Fields Infant School & Nursery we ensure that pupil's wellbeing is continually monitored through discreet PSHE lessons, including Relationships Education, and opportunities where pupils can voice their concerns.
- As part of this learning, pupils will look specifically at online safety relating to screen time use and allowances, and how people's behaviour can differ online and offline.
- These lessons will be conducted in a safe and trusting manner, where pupils will be encouraged to follow the 'SMART' guidance for staying safe online.

Communication of the Policy

To Pupils

- Pupils need to agree to comply with the pupil Acceptable Use of School Computers Policy in order to gain access to our systems and networks and to the internet.
- Pupils will be reminded of the contents of the Acceptable Use of School Computers Policy as part of their Online Safety education.

To Staff

- All staff will be shown where to access the Online Safety Policy and its importance will be explained.
- All staff must sign and agree to comply with the Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy in order to gain access to the school's systems and networks and to the internet.

To Parents

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters.
- Parents will be offered Online Safety training annually.

Mobile Technology Guidance

<u>Staff and Visitors use of personal devices</u>

- Mobile phones and personally-owned devices may not be used during lesson time. They should be switched off (or silent) at all times.
- Mobile phones and personally-owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or devices.
- No images or videos should be taken on mobile phones or personally-owned devices, including on school trips or out of school activity – only school provided equipment will be used for this purpose.
- Staff are not permitted to use their mobile phones or personal devices for contacting pupils, young people or those connected with the family of a student.
- If a member of staff breaches the school's policy, then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to the lunchbreak and after school.

Vulnerable Children

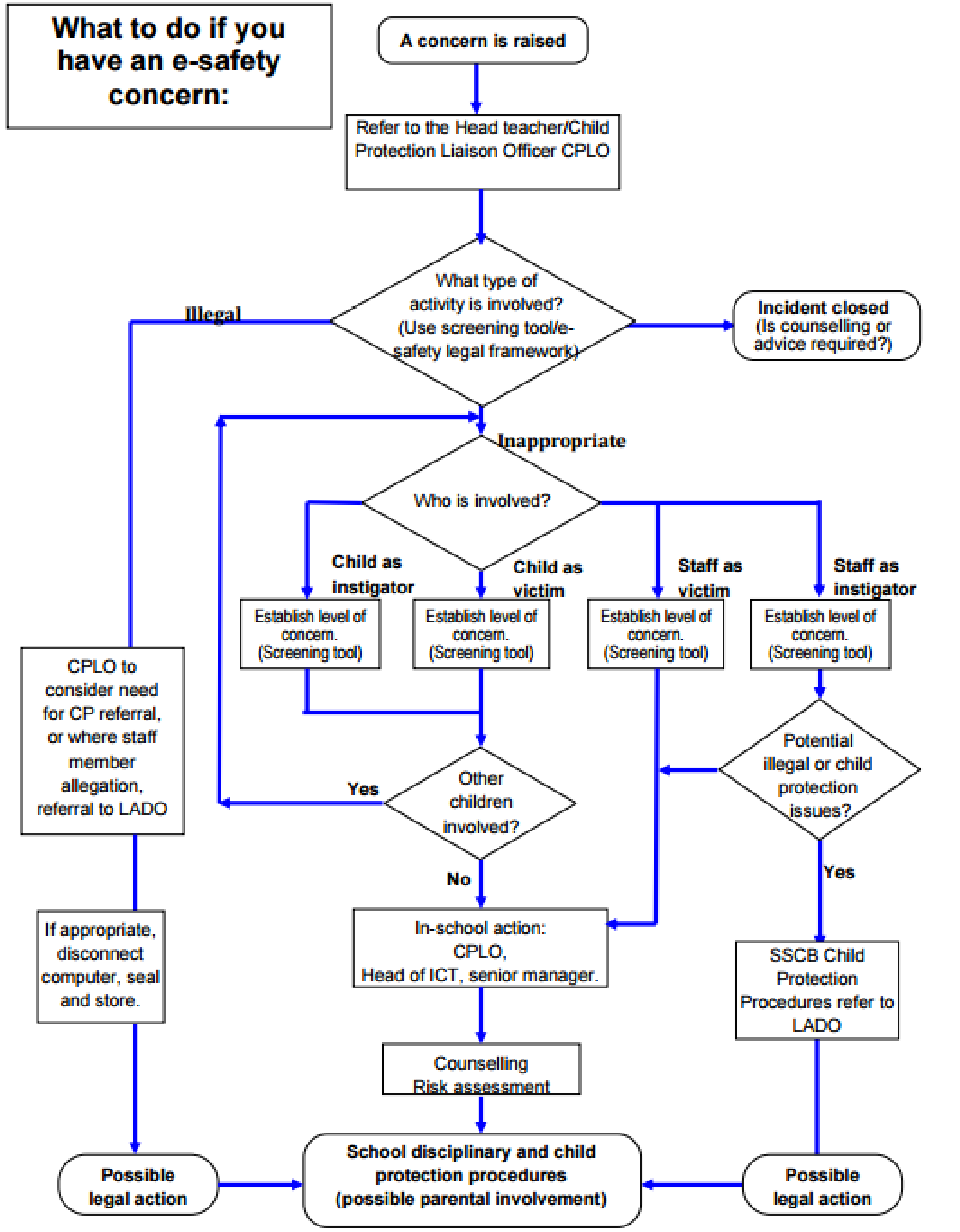
- Any pupil can be vulnerable online and their vulnerability is affected by their age, developmental stage and personal circumstance.
- WFIS recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- WFIS will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum, WFIS will seek input from specialist staff as appropriate, including the SENCO.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Appendix 1

Surrey County Council E-Safety Concern Flowchart



What to do if you have an e-safety concern:
A concern is raised
Refer to the Head teacher/Child Protection Liaison Officer CPLO
What type of activity is involved? (Use screening tool/e-safety legal framework)
Illegal
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
CPLO to consider need for CP referral, or where staff member allegation, referral to LADO
Yes
Other children involved?
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store.
In-school action: CPLO, Head of ICT, senior manager.
SSCB Child Protection Procedures refer to LADO
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement)
Possible legal action

Duty LADO: 01372 833310 (Local Authority Designated Officer)

Contact Centre Children's referrals 0300 200 1006