Byfleet Primary School

Online Safety Policy

Date of Approval	September 2026
Date of Last Review	September 2026
Date of Next Review	September 2027
Signed	**Richard Bowman** Headteacher
Signed	**Joy Considine** Chair of Governors

Aims and objectives

1.1 At Byfleet Primary School we know and understand that the Internet is an important element of modern life for education, business and social interaction. The school understands online safety as an essential part of safeguarding and provides pupils with quality Internet access as part of their learning experience whilst developing digital resilience and online independence.

1.2 The policy considers the DfE statutory guidance Keeping Children Safe in Education (2023), Teaching Online Safety in Schools (DfE 2023), Early Years and Foundation Stage and the Surrey Safeguarding Online Family Centre.

1.3 The purpose of Byfleet Primary School's Online Safety Policy is to:

- Safeguard and protect all members of Byfleet Primary's community online, including online sexual abuse.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

1.4 Byfleet Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into 4 areas of online risk - the 4Cs:

CORE	**Content** Child as recipient	**Contact** Child as participant	**Conduct** Child as actor	**Contract** Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Updating the 4Cs of online risk.

1.3 The purpose of Byfleet Primary School's Online Safety Policy is to:

- Safeguard and protect all members of Byfleet Primary's community online, including online sexual abuse.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly to role model positive behaviour online and to manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns.

1.4 Byfleet Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into 4 areas of online risk - the 4Cs:

CORE	**Content** Child as recipient	**Contact** Child as participant	**Conduct** Child as actor	**Contract** Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

Updating the 4Cs of online risk.

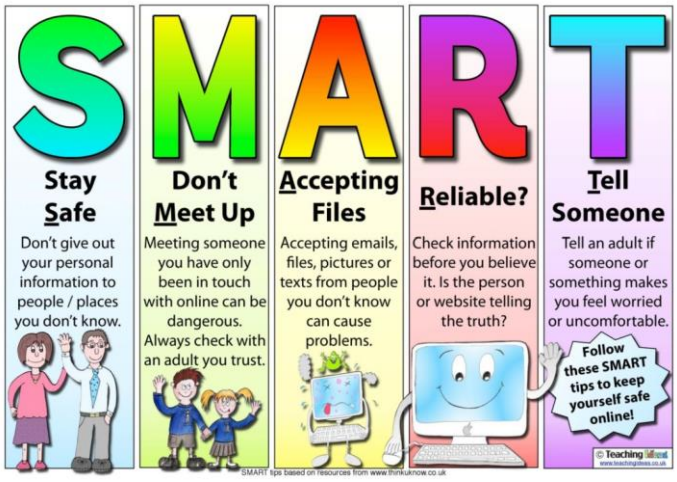
The 4Cs classification recognises that online risks arise when a child:

- engages with and/or is exposed to potentially harmful **CONTENT** (illegal, inappropriate or harmful material)
- experiences and/or is targeted by potentially harmful **CONTACT** (harmful interaction with other users)
- witnesses, participates in and/or is a victim of potentially harmful **CONDUCT** (personal online behaviour that increases the likelihood of, or causes harm)
- is party to and/or exploited by a potentially harmful **CONTRACT** (child as the consumer)

1.5 The school will be guided by the Online Response Guidance document **(Appendix 2)** when dealing with an online risk or incident.

1.6 Any incident involving online safety/inappropriate online behaviour is recorded in the Online Incident Log **(Appendix 3)** and will reference the Online Response Guidance. In most cases, an incident reported involving a 'victim and perpetrator' will automatically be classified at Level 4 on the Behaviour Policy.

1.7 The teaching of Online Safety is supported by:

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for 

Internet use, SMART rules are displayed within the school and referred to during lessons and assemblies.
- The school Internet access is provided by the school contract with Schools Broadband and includes appropriate filtering to ensure our children are safe online. The DSL receives live feedback of any prohibited searches or access to blocked websites so active steps can be taken to address individuals. A weekly SENSO report is analysed by the DSL to spot any trends or possible teaching points.
- Online safety is through the computing curriculum and PSHE curriculum. It is taught for one discreet lesson at the start of each half term and then explored through different themes throughout the rest of the year. For example, the reliability of information (SMART is covered in lesson 3 of the Year 5 Computer Systems unit. See our Computing MTP here)
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

- Pupils will be shown how to publish and present information appropriately to a wider audience.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon and know how to report any online sexual abuse

2. Managing Internet Access

Information system security

- The school's ICT equipment, including online provision, is managed by Eduthing.
- School ICT systems security is reviewed regularly, through SENSO
- Virus protection is updated regularly
- Visitors are required to sign a visitor's agreement prior to use of school online technologies
- Staff must change passwords on a regular basis, or when prompted to do so.
- The school accesses support from Eduthing who provide advice on safer online practices and filtering.

3. Reducing general & Online Risks

Our school recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- Adults are vigilant during Computing lessons to ensure that the materials being accessed, and devices being used, are appropriate and in line with this policy. Any incident which causes concern, is reported following the appropriate channels depending on the nature of the incident.
- Educating our children about using CEOP button on our website to report anything concerns about online sexual abuse & ensuring children know the school will not tolerate reports of online sexual abuse, and will take the matter very seriously, involving parents/carers, Youth Offending Team and the Police where necessary.
- 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 SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective. We complete annual Online safety /ICT usage questionnaires.

4. Email

- Pupils and staff may only use approved google @byfleetprimary.sch.uk e-mail accounts on the school system and must immediately tell a teacher or Online Safety leader if they receive offensive email.
- Staff must not reveal personal details of themselves or others, or confidential information about school in email communication, websites (including social networking sites) or in chat rooms.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters is not permitted.
- Communication between parents and staff will be via info@byfleet.surrey.sch.uk or head@Byfleet.surrey.sch.uk

5. Remote access

- All teachers should access emails and documents including photographs and videos via the school remote access Google Drive and G Suite software package.
- Google Classroom is accessible for parents and children remotely.
- Guidance is published on each Google Classroom page to ensure that children and adults are aware of how to use this software appropriately and effectively.
- Adult names are visible on Google Classroom to ensure transparency around adults' users.
- Parents are encouraged to use other communication channels to contact adults.
- As part of our Online Safeguarding procedures, we ensure all messages are typed without anonymity which enables us to identify the adult user and maintain familiarity for the children.

Google Classroom Guidance summarised and visible on each classroom.

This Google Classroom is an excellent tool for our children to engage with their learning and keep the adults they work with up to speed with their learning, both on and offline. As a school we will use Google Classroom to send out messages to year groups which are specific to them, comment on work and signpost resources which might enhance the learning of the child. The email addresses and names of adults are visible for safeguarding purposes but please contact the school office directly through info@byfleet.surrey.sch.uk if you have a specific query or question for a member of staff.

Children are welcome to comment on here by:
- Using full sentences and correct punctuation.
- Writing messages which show our school values of Ready, Respectful, Safe.
- Making sure the messages are about their learning.

- Explain their ideas and the point of the message clearly.

6. Published content and the school website

- The contact details on the school's website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.
- The head teacher and Website Leader will take overall editorial responsibility and ensure that content is accurate and appropriate.

7. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.
- Pupils' full names will be avoided on the school's website, including in blogs, and will not be used in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Parents sign a consent form when their child starts school to give permission for photographs to be shared online or in the media.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Byfleet Primary School recognises that Online Safety is an essential part safeguarding of our pupils both in school and at home.

8. Vulnerable Pupils

- Our school is aware that some pupils 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.
- Our school will ensure that an adapted and ability-appropriate online safety education, access and support is provided to vulnerable pupils.
- Byfleet Primary School will seek input from specialist staff as appropriate, including the Inclusion leader and DSL.

9. Social Networking

- The school will control access to social networking sites and consider how to educate pupils in their safe use e.g. use of passwords and blocking those who elicit inappropriate behaviour like unkindness.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils
- Pupils will be advised to use nicknames and avatars when using social networking sites.

- Pupils will be taught through Computing Lessons, through PSHE lessons and through regular assemblies and themed days such as 'Safer Internet Day' about how to report online sexual abuse.

10. Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Lead.
- The Online Safety Lead, in conjunction with Eduthing (the School's ICT management and technical support provider) will ensure that regular checks are made to ensure that the filtering methods (SENSO) selected are appropriate, effective and reasonable.
- The school makes use of LGFL's Filter Test regularly, to check filtering is appropriate.

11. Use of personal devices including Smart Phones:

- Staff are required to lock personal phones in drawers during teaching hours.
- Staff should not contact parents directly using their personal phone (even on private number) but should instead go through the school office.
- Children are not permitted to bring their personal mobile technology into school. However, this is at the discretion of the head teacher. Year 5/6 pupils who walk home alone may be permitted to bring a phone, however this must be labelled and kept in a locked cupboard during the day. All mobile phones are turned off at the school gate before entering and may only be turned back on at the end of the day upon exiting the school gate. A mobile phone/device agreement is made with each parent who has signed up and agreed to adhere to the rules of phone use, which may be reviewed at the Headteacher/DSL's discretion.
- Personal Smart phones must never be used to take photographs of pupils. A Mobile Phone, Smartwatch, Electronic Devices & Camera policy can be found here.

Staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable, including pornographic images of children, without deleting them.

Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's behaviour policy. The school follows the DFE 2022 guidance '***Searching, screening and confiscation***'.

12. Parents as employees

- It is acknowledged that some staff also have children who attend the school. It is recognised that in these cases the staff fulfil a dual role of parent and employee.
- Parents as employees should ensure that they uphold boundaries between the two roles and that their behaviour does not constitute a conflict of interest. For example, they must maintain the same level of confidentiality despite social expectations. Parent-staff should discuss any inter-role conflict with their line manager.
- At Byfleet Primary School our policy is that staff who are also parents should make a clear distinction between their personal account and staff account and therefore preserve the privacy of other staff working at the school. They should adhere to the high expectations the school has for their personal conduct online. Details of grievance procedures related to staff inappropriate online behaviour can be found in the Staff Handbook.

13. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and 2003.

GDPR

If you have any questions about how we handle your personal information, please contact the School Business Manager. If you need further information, please contact the Data Protection Officer: Craig Stilwell email: dataservices@judicium.com

14. Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

15. Handling Online safety concerns & complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the head teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaint's procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

16. Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school Online Safety Policy.

17. Introducing the Online Safety Policy to pupils

- The children sign an Acceptable Use Policy annually which is displayed in their classrooms.
- Children are taught explicitly within Computing sessions, assemblies, PSHE and circle time, about how to stay safe online.
- Sanctions for inappropriate use of ICT by pupils will be dealt with using our school Online safety rules and sanctions (Appendix 5)
- Appropriate elements of the Online Safety Policy will be shared with pupils.
- Online safety rules will be posted in all rooms with computer access.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of Online safety issues and how best to deal with them will be provided for pupils.
- Pupils will celebrate Safer Internet Day in February of each year in addition to Online safety lessons integrated into lessons throughout the year (following curriculum).

19. Staff and the Online Safety Policy

- All staff have access to the School Online Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Sanctions for inappropriate use of ICT by staff will be dealt with in line with the Disciplinary and Capability policy, with advice from the LADO where appropriate.

20. Enlisting parents' support

- Parents' and carers attention will be drawn to the School Online Safety Policy in newsletters, the school prospectus and on the school website
- Parents and carers will from time to time be provided with additional information on Online safety
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school
- The school works with an online safeguarding company to support its parents about Online Safety, ensuring parents are kept up to date.
- This policy will be approved by the Governing Body and reviewed at least annually.

APPENDIX 1 - Staff, Governor and Visitor Acceptable Use Agreement / ICT Code of Conduct

Byfleet Primary School

Staff Acceptable Use Policy / ICT 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. The school uses G-Suite. 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 always adhere to its contents to keep each other safe.

➢ I appreciate that ICT includes a wide range of systems, including mobile phones, mobile watches, digital cameras, email, social networking and that ICT use may also include personal devices when used for school business.

➢ I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. Due to the confidential and sensitive nature of information shared via ICT, Byfleet ICT systems (log ons, email accounts etc.) may only be used by the assigned member of staff and may not be viewed or accessed by others i.e. **family members.**

➢ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

➢ I understand that I am responsible for all activity carried out under my username.

- ➢ I will only use the school's email / internet / Google Classroom and G-Suite and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.

➢ I will only use the approved, secure Google email system (GMAIL) for any school business.

➢ I will ensure that personal data (such as data held on scholarpack/CPOMS) is kept secure 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 teacher or Governing Body.

➢ I will not install any hardware or software without the permission of the Head.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

- 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 the Head teacher. SENSO is used for monitoring, which I have been made aware of.

- I will respect copyright and intellectual property rights.

- 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/learning platform without the permission of the parent/carer, member of staff or Head teacher.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

- I will ensure that all electronic communications with parents, pupils and staff, including email and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. This includes abiding by the Whatsapp Code of Conduct.

- I will support the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

- I will report any incidents of concern regarding children's safety to the Online Safety Lead, a DDSL, DSL or Head teacher.

- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school. This document has been uploaded onto CPOMS and acknowledged to be read, understood and agreed to be complied with.

Full Name:…… …… (Printed)

Job title:…… ……

Date: ……..

Signature……

APPENDIX 2 - Online Response Guidance

Online Response Document

APPENDIX 3 - Online safety Incident reporting log

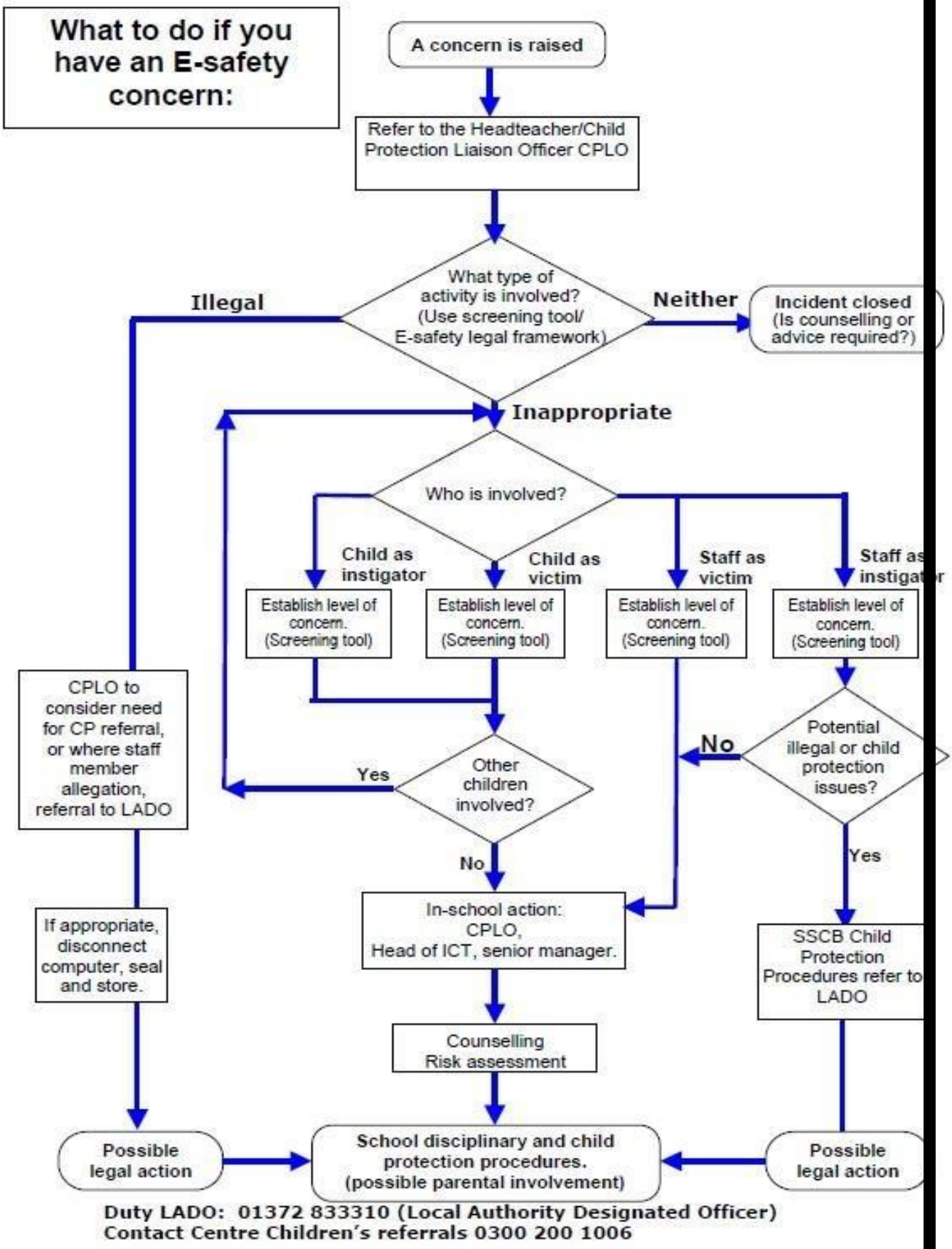
Online Safety Lead	
	ard Bowman, Kirsten Hurford and Rebecca Partridge
gory of incident)	
e	Date
ription of incident	

Did the incident involve material being	Created Viewed Printed Shown to other Transmitted to others Distributed
Could this incident be considered as	Harassment Grooming Cyberbullying Sharing of nudes/semi-nudes (self-taken indecent imagery) Breach of AUP er (please specify) _
on taken	f Incident reported to head teacher/senior manager Advice sought from children's social care Incident reported to police Incident reported to CEOP incident reported to Internet Watch Foundation Incident reported to IT iplinary action to be taken ne policy to be reviewed/amended d/young person  dent reported to member of staff (specify) dent reported to social networking site incident reported to IT Child's parents rmed iplinary action taken child/young person debriefed

	ne Safety Policy to be reviewed/amended

Outcome of incident/ investigation

Children's social care	
Police/CEOP	
Organisation	
Individual (staff member/child)	
Other (HR/legal etc)	
Children's social care	


What to do if you have an E-safety concern:
A concern is raised
Refer to the Headteacher/Child Protection Liaison Officer CPLO
What type of activity is involved? (Use screening tool/ E-safety legal framework)
Illegal
Neither
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)
Potential illegal or child protection issues?
No
Yes
Other children involved?
Yes
No
CPLO to consider need for CP referral, or where staff member allegation, referral to LADO
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

APPENDIX 5

Pupil Online Safety rules and sanctions

It is appropriate for people to be allowed a great deal of freedom in using ICT for study, work and leisure. With freedom comes responsibility. Byfleet Primary School cannot control what people, all over the world, make available on the Internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form. If material is considered to be unacceptable by the school when presented in a book, magazine, video, audio tape or spoken form, then it is not acceptable on the ICT network.

We expect all ICT users to take responsibility in the following ways:

Not to access or even try to access any material which is:

- Violent or that which glorifies violence
- Criminal, terrorist or glorified criminal activity (including drug abuse)
- Racist or designed to incite racial hatred
- Of extreme political opinion
- Pornographic or with otherwise unsuitable sexual content
- Crude, profane or with otherwise unsuitable language
- Blasphemous or mocking of religious and moral beliefs and values
- In breach of the law, including copyright law, data protection, and computer misuse
  • Belongs to other users of ICT systems and which they do not have explicit permission to use
- Not to search for, or use websites that bypass the school's Internet filtering
  • Not to download or even try to download any software without the explicit permission of a member of the ICT systems support department
  • Not to attempt to install unauthorised and unlicensed software
- To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers
- Not to use other people's user ID or password, even with their permission
- Not to interfere with or cause malicious damage to the ICT Facilities
- To report any breach (deliberate or accidental) of this policy (to the headteacher) immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Byfleet Primary reserves the right to access all material stored on its ICT system, including that held in personal areas of staff and pupil accounts for purposes of ensuring DCFS, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the ICT facilities.

Byfleet Primary will act strongly against anyone whose use of ICT risks bringing the school into disrepute or risk the proper work of other users. Persistent offenders will be denied access to the ICT facilities – on a permanent basis.

Sanctions for the misuse of Byfleet Primary ICT facilities

First Offence

- The pupil will have a conversation with the Online Safety Lead to discuss the breaking of the ICT AUP.
- The pupil will need to read the ICT AUP to ensure they are clear about the expectations.
- The Online Safety Lead will write a letter to parents (or phone if required) to inform them of the breaking of the ICT AUP.
- The pupil may receive a further sanction depending on the nature of the offence.
- The relevant staff will be informed.

Second Offence

- The Online Safety Lead will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the second time. The letter may include specific information about the offence.
- The pupil may receive a further sanction depending on the nature of the offence.

- The relevant staff will be informed.

Third Offence

- The pupil will have their email and/or Internet access removed immediately by the Online Safety Lead for a minimum of 2 weeks.
- Online Safety Lead will write a letter to parents and phone them to inform them of the breaking of the ICT AUP for the third time. The letter will ask parents to come into school to discuss the breaking of the ICT AUP with the Online Safety Lead.
- The pupil will have a meeting with the Online Safety Lead and the Headteacher to discuss the breaking of the ICT AUP and the subsequent sanction.
- The relevant staff will be informed.

Considerations will be made in line with the school behaviour and exclusion guidance where appropriate. It should be noted that if a pupil puts themselves, other pupils or a member of staff in danger by giving out personal details they will be banned from using the ICT facilities for a fixed period of time and if required the police will be informed.