MAYBURY PRIMARY SCHOOL

Online Safety Policy

Updated: Autumn 2018

Key Details

Designated Safeguarding Lead (s): Amanda Merritt. Della Sullivan

Named Governor with lead responsibility: Christine Cornish

Online Safety Leader: Rachel Frew

Date written: October 2018

Date agreed and ratified by Governing Body:

Date of next review: October 2019

This policy will be reviewed at least annually.

It will also be revised following any concerns and/or updates to national and local guidance or procedure

Maybury Primary School

Produced : Autumn 2014
Reviewed : Autumn 2018
To be reviewed: Autumn 2019

Online Safety Policy

Mission

Our values-based school nurtures curiosity and creativity through an inspiring, broad and engaging curriculum, where learning is at the heart of all that we do. Our children learn to become resilient and self-assured in an environment where safety is outstanding. Everyone is challenged and encouraged to thrive and achieve as individuals, preparing them for their role as caring and active citizens in modern Britain.

Vision statement

"Everyone is a learner and every experience is a learning opportunity."

1 Aims and objectives

This online safety policy has been written by Maybury Primary School involving staff, pupils and parents/carers,

1.1 At Maybury we understand the Internet is an important element in 21st century 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 takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2018, Early Years and Foundation Stage 2017 and the Surrey Safeguarding Children Board procedures.

1.3 The purpose of Maybury Primary School's online safety policy is to:

- Safeguard and protect all members of Maybury Primary's community online.
- 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 Maybury Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use, SMART rules are displayed around the school.
- The school Internet access is provided by the school contract with Schools Broadband and includes appropriate filtering to ensure our children are safe online
- 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

2. Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Visitors are required to sign a visitors agreement prior to use of school online technologies
- Staff must change passwords on a regular basis
- The school accesses support from Softegg who provide advice on safer online practices and filtering.

3. Reducing 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.

4. E-mail

- Pupils and staff may only use approved e-mail accounts on the school system and must immediately tell a teacher or Online Safety co-ordinator if they receive offensive e-mail.
- Staff must not reveal personal details of themselves or others, or confidential information about school in e-mail communication, websites (including social networking sites) or in chat rooms.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. The forwarding of chain letters is not permitted.

- Pupils use Purple Mash email tools which teaches them about the structure of emails
- Communication between parents and staff will be via info@maybury.surrey.sch.uk or head@maybury.surrey.sch.uk

5. Remote access

All teachers should access emails and documents including photographs and videos via the school remote access and shared drives.

6. Published content and the school web site

The contact details on the Web site 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 Web site, 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 Web site. 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.

Maybury 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 considered to be 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 differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.

Maybury Primary School will seek input from specialist staff as appropriate, including the Inclusion leader and Designated Teacher.

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

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 encouraged to report any problems they encounter if using any social networking site and these will be reported in the Online Safety log book.

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 Soft Egg (the School's ICT management and technical support provider) will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

The school uses software, 'Future Digital', to monitor computer based activities on pupil and staff logins. This is monitored weekly by the head teacher.

11. Use of personal devices including Smart Phones:

Staff are required to lock personal phones in drawers or safes 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 6 pupils who walk home alone may be permitted to bring a phone, however this must be labelled and kept in the school office during the day.

Personal Smart phones must never be used to take photographs of pupils.

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 2018 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 Maybury 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.

13. Protecting personal data

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

GDPR
We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by the School Business Manager, then you can contact the DPO on the details below: -

Data Controller Name: Craig Stilwell
Data Controller Details: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Data Controller Email: dataservices@judicium.com

14. Authorising Internet access

All staff must read and sign the 'Staff Code of Conduct for ICT ' (Appendix 1) 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.

Any person working on school premises using the school network will be asked to read and adhere to an '**Visitor Notice- ICT Acceptable Use / Code of Conduct '** form (Appendix 2) before being allowed access to the Internet. Visitors to the school will be provided with a guest username and password to log on to the school network, which will allow limited access to files and programs.

All persons accessing the school system will need to agree to Future Digital settings before being allowed access.

15. 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 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.

16. Handling Online safety 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 complaints procedure.

Pupils and parents will be informed of consequences for pupils misusing the Internet.

17. **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.

18. Introducing the Online safety policy to pupils

The children sign an Acceptable use policy annually which is displayed in their classrooms.

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 via the S drive and school website and its importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is 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 advise 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 brochure and on the school web site

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 Online Safety Lead will deliver annual parent workshops covering Online safety to ensure 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

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

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

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

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

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

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.

- I will only use the approved, secure email system(s) for any school business.

- I will ensure that any personal devices including laptops, desktops, mobile phones and tablets which has access to professional e-mail and documents is password protected.

- I will ensure that personal data is kept secure and is used appropriately on the school site and not taken off the school premises. **The use of memory sticks or portable devices is strictly prohibited**.

- I will not install any hardware of software without the permission of the ICT leader.

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

- 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 understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will respect copyright and intellectual property rights.

- I will ensure that my online activity (including the use of social media sites), both in school and outside school, will not bring my professional role into disrepute.

- I will report any incidents of concern regarding children's safety to the ICT lead, the Designated Safeguarding Lead or Head teacher.

- I will ensure that electronic communications with pupils including email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- 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 ensure that phone calls made to parents are made on a school phone using 'line 1' or 'line 2' and NOT on a personal device. If on a school trip or residential and a parent needs to be phoned the code '141' must be used before dialing to ensure privacy of personal phone number.

User Signature

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

Full Name……(printed)

Job title……

Signature…… Date……..

Headteacher… AMANDA MERRITT ……..

Signature…… Date……..

APPENDIX 2
Visitor Notice- ICT Acceptable Use / Code of Conduct

All visitors who are using school 'WiFi' or school ICT equipment ('The Service') are required to read the terms and conditions, as set out in this Acceptable Use/Code of Conduct. When you sign into school or start using 'The Service', you are deemed to have read, understood and agreed to the contents of this Acceptable Use/Code of Conduct. Any concerns or clarification should be discussed immediately with the school office, and before using 'The Service'.

- I will only use the school's Internet and any related technologies for professional purposes.

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

- I will ensure that personal data is kept secure and is used appropriately on the school site and not taken off the school premises. **The use of memory sticks or portable devices is strictly prohibited** (except for school's memory stick use for the Smart Table only)

- I will not install any hardware of software without the permission of the ICT leader.

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

- 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 understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the ICT lead, the Designated Child Protection Officer or Head teacher.

APPENDIX 3
Online safety Incident reporting log

Online Safety Lead	Rachel Frew		
DSL	Della Sullivan, Amanda Merritt or Becky Butler		
Details of incident			
Time		Date	
Description of incident			
Name and contact details of person reporting incident			
Who was involved in the incident	child/young person staff member other (please specify _____		
Names and contact details of those involved			
Type of incident	bullying or harassment online bullying or harassment (cyberbullying) sexting (self-taken indecent imagery) deliberately bypassing security or access hacking or virus propagation racist, sexist, homophobic religious hate material terrorist material other (please specify) _____		
Nature of incident	deliberate access accidental access		

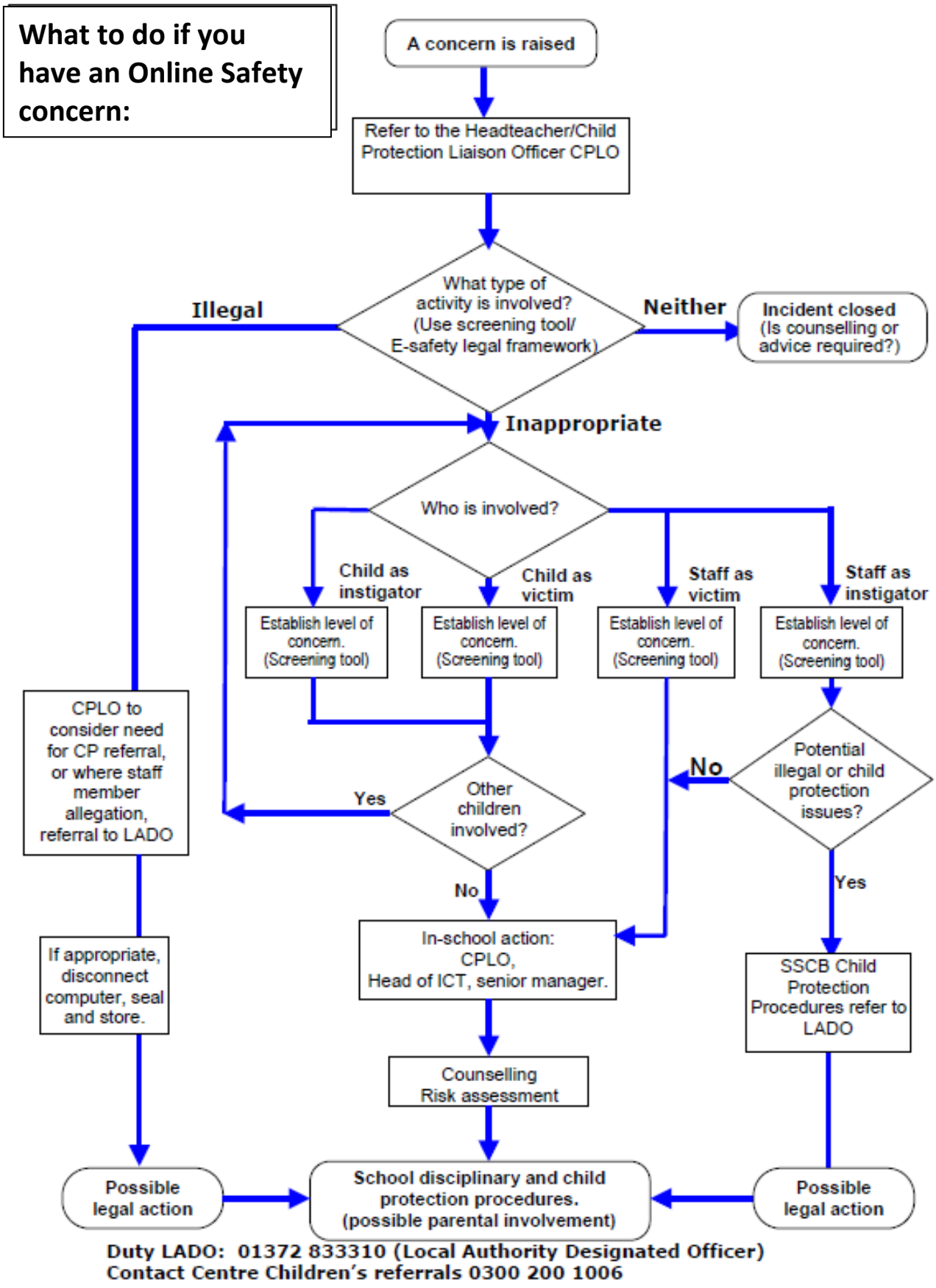
Did the incident involve material being	created viewed printed shown to other transmitted to others distributed
Could this incident be considered as	harassment grooming cyberbullying sexting (self-taken indecent imagery) breach of AUP other (please specify) _____
Action taken	staff incident reported 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 disciplinary action to be taken e-safety policy to be reviewed/amended child/young person incident reported to member of staff (specify) _____ incident reported to social networking site incident reported to IT child's parents informed disciplinary action taken child/young person debriefed e-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	

Learning Points/ Recommendations and timescales to implement

Recommendation 1		Timescale to be implemented	
Recommendation 2		Timescale to be implemented	
Recommendation 3		Timescale to be implemented	
Recommendation 4		Timescale to be implemented	



Responding to an Online Safety incident

This is guidance for senior management within schools, regarding how to respond to an Online Safety incident of concern. It is important to note that incidents may involve an adult or child as the victim or the instigator. Adults are also subject to cyber bullying by pupils.
The first section outlines key Online Safety risk behaviours. The flowchart on page 4 illustrates the approach to investigating an incident of concern. This diagram should be used with the screening tool (page 5) and the Surrey Child Protection Procedures which include what to do if you are concerned about a child, or about an adult working with children. Schools CPLOs will be conversant with these and the processes for referral. They are available on the SSCB website at:

http://www1.surreycc.gov.uk/cafis/manual/index.html
Appendix A provides examples of Online Safety **incidents**, suggests actions to address these risks, and example responses to such incidents.

What are the Online Safety risks?
The rapid growth in technology over the last 10 years, in particular the Internet, has provided endless opportunities for children, young people and adults to gain access to information and to communicate with each other. The Internet is an unmanaged, open communications channel, via which anyone can send messages discuss ideas and publish material – and it's these very features which make it an invaluable resource used by millions of children everyday.

But it is these same features which present a number of risks to children. The vast majority of children's experiences will be positive - but we must be aware that this new technology can be used to bully others, and be manipulated by people who wish to do harm to children.

What does electronic communication include?
- **Internet collaboration tools** (e.g. social networking sites, blogs)
- **Internet Research** (e.g. web sites, search engines and Web browsers)
- **Mobile Phones and personal digital assistants**
- **Internet communications** (e.g. E-mail and Instant Messaging)
- **Webcams and videoconferencing**

Risk Behaviours:
Online grooming and child abuse
There are a number of illegal actions that adults can engage in online that put children at risk:
• Swapping child abuse images in chat areas or through instant messenger with other adults or young people and forming networks with other child abusers to share tips on how to groom more effectively and how to avoid being caught
• Swapping personal information of children that they have collected with other abusers
• Participating in online communities such as blogs, forums and chat rooms with the intention to groom children, collect sexually explicit images and meet them to have sex

Inappropriate or illegal content
Because it's so easy to upload information onto the Internet, much online content is now inaccurate or extreme – yet is often presented as fact. A great deal of the material on the Internet is published for an adult audience, and some is unsuitable for children. For example, there is information on weapons, crime and racism, access to which would be much more restricted elsewhere.
Disclosing personal information and identity theft
Publishing personal information about themselves online could compromise children's security, and that of those around them. Furthermore, as soon as a message is sent or an image is posted, it can be shared, copied and changed by anyone. Children need to think carefully about their online 'etiquette'.

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. Maybury 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. Maybury 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.

Maybury 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 Maybury Primary ICT facilities

First Offence

• The pupil will have a conversation with the Online Safety Co-ordinator 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 Co-ordinator 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 Co-ordinator 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 Co-ordinator for a minimum of 2 weeks.
• The Online Safety Co-ordinator 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 Co-ordinator.
• The pupil will have a meeting with the Online Safety Co-ordinator 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.