

Waterloo Primary School



Acceptable Use Policy

Approved by: S Robinson – Chair of Governors

Signed: 

Review date: September 2024

Contents

Introduction

Roles and Responsibilities

E-Safety in the Curriculum

Password Security

Data Security

Managing the Internet safely

Mobile Technologies

Managing email

Safe Use of Images Misuse

and InfringementsEqual

Opportunities Parental

Involvement

Writing and Reviewing this Policy

Appendices

Acceptable Use Agreement: Staff, Governors and Visitors

Acceptable Use/E-Safety/Remote Learning Agreement:

Pupils & Parents

Smile and Stay Safe Poster

Flowchart for Managing E-Safety Issues

Current Legislation

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Waterloo Primary School we understand the responsibility to educate our pupils on safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.)

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.

Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named E-Safety co-ordinator in our school are **Craig Otten**

The Data Protection School Lead is **Lindsay McCarthy**

The Data Protection Officer is **Peter Rafferty (Row7Education)**

It is the role of the E-Safety co-ordinators to keep abreast of current issues and guidance through organisations such as Sefton LA, Becta, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the Head/ E-Safety co-ordinators and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the GDPR and School Data Protection policies and the school's acceptable use agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school-child agreement, home learning, behaviour (including the anti-bullying) policy and PSHE.

E-Safety skills development for staff

- Our staff receive regular information and training on E-Safety issues in the form of staff meetings and notices.
- Details of ongoing staff training is available from the E-Safety co-ordinators
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community (see attached flowchart.)
- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas as identified on year group curriculum maps and whole school curriculum subject advisor overviews.

Managing the school E-Safety messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The E-Safety policy will be introduced to the pupils at the start of each school year.
- E-Safety posters will be prominently displayed.

ESafety in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about E-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils have access to activities on Internet safety.
- Parents have access to E-Safety support on our website
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- E-safety lessons are included in our PSHE curriculum maps and our computing curriculum maps. Opportunities to embed and extend this learning are provided through anti –bullying week and E-Safety Week.

Password Security

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy.
- Users are provided with a Learning Platform log-in username. They are also expected to use a personal password and keep it private.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the School Business Manager
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, systems and the Learning Platform, including ensuring that passwords are not shared and are changed periodically
- Due consideration should be given to security when logging into the Learning Platform to the browser/cache options (shared or private computer)

Data Security

The accessing of school data is something that the school takes very seriously.

Staff are aware of their responsibility when accessing school data. They must ensure that:

- Data accessed outside of school is password protected
- Copies of data is kept securely
- Others do not view data outside of school
- Data isn't edited unless specifically requested to do so by the Headteacher and/or Governing Body.

Managing the Internet

The Internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils. Google images is only accessible to staff
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastructure

- Agilisys monitor web-based activity and school internet access is controlled through them and Sefton Local Authority.
- Our school has the facility for additional web filtering which is agreed upon and monitored by our Computing Advisory Teacher in liaison with the technician from Agilisys.
- Waterloo Primary is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, (Agilisys in conjunction with Helen Owens (School Business Manager) to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.
- Pupils and staff have limited ability to download programs or files on school based technologies.

- If there are any issues related to viruses or anti-virus software, the E-Safety co-ordinator should be informed.

Mobile Technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Pupils are taught how to use mobile technologies outside of the school setting safely and staff will respond appropriately where concerns for misuse outside of the school setting are raised.

Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Members of staff should not contact a pupil or parent/carer using their personal device (unless they know the parent in a personal context and it is non-work related or unless permission is given by the Headteacher and their number is withheld)
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Personal devices should only be switched on and used when staff are not in contact with pupils unless they have been given consent by the Headteacher
- Pupils are not permitted to use personal mobile devices when on school premises. Devices must be switched off and left at the school office.

School provided Mobile devices (including phones)

- Some staff are provided with a mobile phone and there is a school mobile phone for the purposes of trips
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on

- the devices of any member of the school community.
- Where the school provides mobile technologies for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Managing Email

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Staff who require to send or receive confidential emails will be assigned an Egress account.

Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. Pupils must have experienced sending and receiving emails in order to develop this skill.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoid the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder.
- E-mails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations, parents or pupils are advised to cc a relevant member of staff into the email.
- Pupils may only use school approved accounts on the school system and for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

- Staff must inform the Headteacher if they receive an offensive e-mail
- Pupils are introduced to email as part of the Computing Scheme of Work

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing pupil's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- on the school's Learning Platform
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- on school authorised social media accounts e.g. Twitter

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents (where there is joint custody) in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Pupils names and images will only be viewed together when access Google Meet which is a secure learning platform.

Images may be uploaded to the website by any member of staff with access rights provided that they have checked the consent lists to ensure that they are not in breach of parent authorisation.

Storage of Images

- Images/ films of children are stored on the School Google shared drive or school staff shared drive
- Pupils and staff are not permitted to use personal portable media for storage of pupil images (e.g. USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.
- Images should be deleted when they are no longer required, or the pupil has left the school. Helen Owens (Data Protection Officer) will check that this has been done on an annual basis.

Webcams and CCTV

- Webcams in school are only ever used for specific learning purposes
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences through the Home/School Acceptable Use Agreement
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils are supervised by a member of staff when video conferencing from school
- All pupils are supervised by a member of staff when video conferencing from school with end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only

- switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.
- Google Meet is used for the purposes of remote teaching and staff meetings where staff/pupils are not on school premises. Only those invited to the Meets are able to attend.

Additional points to consider:

Participants in conferences offered by 3rd party organisations may not be DBS checked but conferencing will be supervised by an adult.

Conference supervisors need to be familiar with how to use the video conferencing equipment; how to end a call if at any point any person taking part becomes unhappy with the content of the conference; how to block/remove a participant if their conduct is inappropriate.

There must be a minimum of three children on a Google Meet or an additional member of staff present.

Misuse and Infringements

Complaints

Complaints relating to E-Safety should be made to an E-Safety co-ordinator or Headteacher. Incidents should be logged and the **Flowcharts for Managing an E-Safety Incident** should be followed (see appendix).

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to an E-Safety co-ordinator or DSL.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator or DSL, depending on the seriousness of the offence; investigation by the Headteacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct on the **Acceptable Use Agreement**.

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents/carers and pupils are actively encouraged to contribute to the school E-Safety policy by letter and by reporting unsuitable sites etc. to the E-Safety co-ordinator
- Parents/carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to E-Safety where appropriate in the form of;
 - Website/ Learning Platform postings
 - Newsletter items

Writing and Reviewing this Policy

The policy is available to all stakeholders and the agreement/code is signed by anybody coming onto the premises.

Review Procedure

There will be an on-going opportunity for staff to discuss with the E-Safety coordinators or a DSL any issue of E-Safety that concerns them.

This policy will be reviewed every 12 months (or more frequently if required) and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Waterloo Primary School Acceptable Use Agreement/Code of Conduct: Staff, Governors and Visitors

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 Craig Otten** the school E-Safety coordinators or **Lindsay McCarthy** the Data Protection Officer.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

I will only use the school's email / Internet / Intranet / Learning Platform 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 will ensure that all electronic communications with pupils and staff are compatible with my professional role.
 I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
 I will only use the approved, secure email system(s) for any school business.
 I will ensure that personal data (such as data held on SIMS) 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 or Governing Body.
 I will not install any hardware or software without seeking permission from the Headteacher.
 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 without the permission of the parent/carers, member of staff or Headteacher.
 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 Headteacher.
 I will respect copyright and intellectual property rights.
 I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
 I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
 I give permission for my photograph to be used for school purposes - where appropriate (website, Twitter, school displays, press, external agencies/partners)
 I will ensure that any external devices (portable hard drives, USB devices etc. are encrypted) I will adhere to policy and procedures set out in the safeguarding policy and addendum

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school for internal and remote learning and purposes.

Signature Date

Full Name(printed) Job title



Pupil & Parent Acceptable Use, ESafety and Remote Learning Agreement

- I will only use ICT in school for school purposes
- I will only use school devices allocated for school purposes
- I will only use my school email address when emailing in school and will only use it for school purposes when communicating with staff or other pupils.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell a member of staff immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone
- I will be responsible for my behaviour when using ICT both in and out of school, because I know that these rules are to keep me safe
- I will follow the guidance and rules of conduct shared by staff when accessing Google Meets
- I will not screenshot, photograph or record Google Meets
- I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my E-Safety
- I will ensure that I am appropriately dressed for virtual learning
- I understand that my child's full name and image will appear when they are in the Google Meet which is a secure learning platform that can only be accessed with permission from the host.
- I understand that it is my responsibility to ensure that my child's internet use is supervised and/or that suitable parental controls are in place

Pupil Name/s: _____ Pupil Class/es: _____

Pupil Signature: _____

I will support my child/ren in adhering to the agreement above and the SMILE protocol and will ensure that my child/ren and I follow the Acceptable Use and Remote Learning Policies.

Parent Name: _____ Parent Signature: _____ Date: _____



REMEMBER -SMILE

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

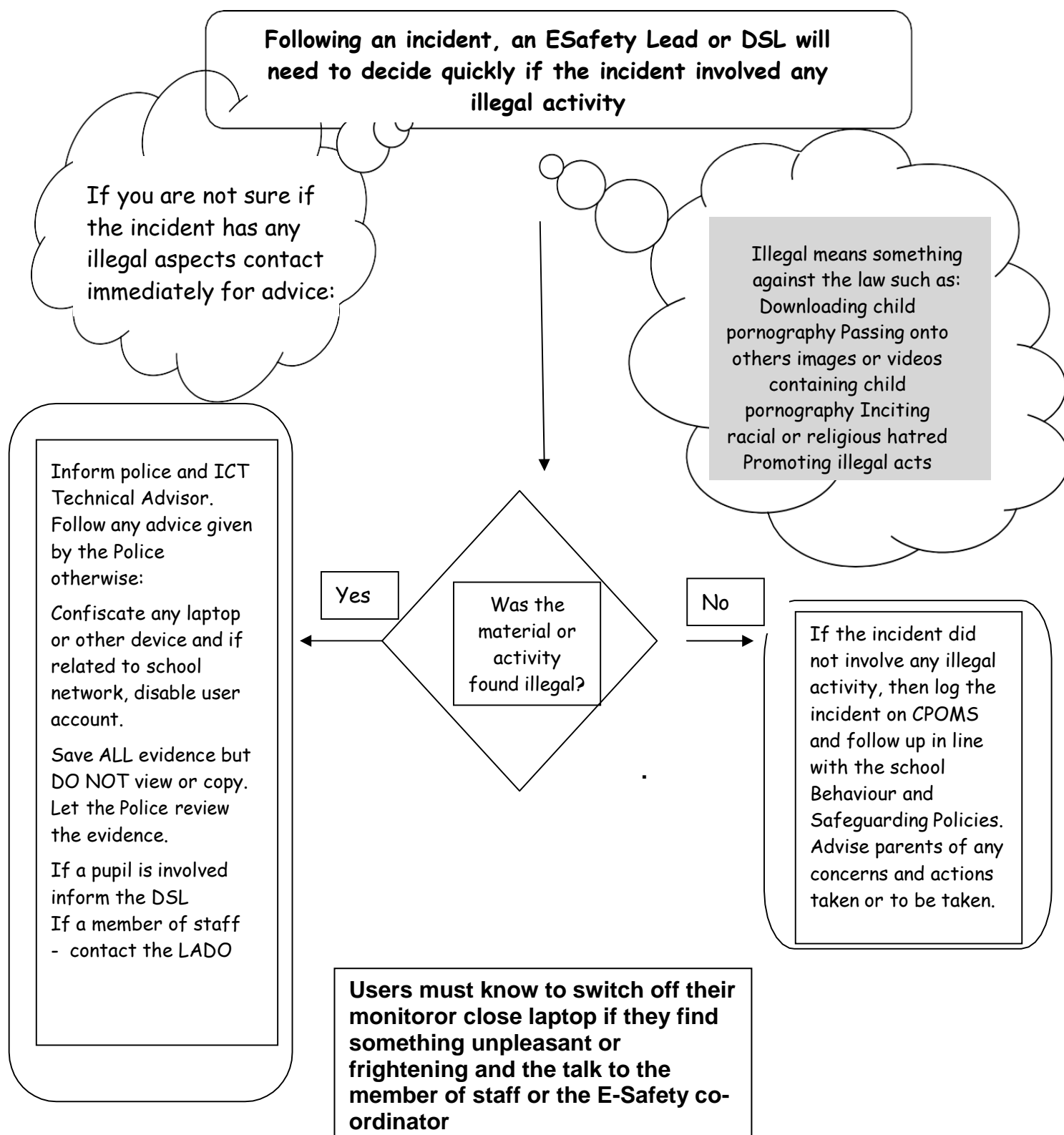
Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Flowchart for Managing an E-Safety Incident



Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hmso.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

Human Rights Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980042.htm>

Other Acts relating to E-Safety

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.

Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

For more information

www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose

Appendix

of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions