Isle of Ely
PRIMARY SCHOOL

E-safety Policy

The Acceptable Use of the Internet and related Technologies

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the *Governing Body on:*	July 2015
The implementation of this e-safety policy will be monitored by the:	*Headteacher*
Monitoring will take place at regular intervals:	*Every six months*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Annually*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	July 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Active Learning Trust, LA ICT Manager, LA Safeguarding Officer*

The school will monitor the impact of the policy using: *(delete / add as relevant)*

- *Logs of reported incidents*
- *LGfL monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity (Beebug)*
- *Surveys / questionnaires of*
  - *pupils (e.g. Ofsted "Tell-us" survey / CEOP ThinkUknow survey, LGfL Survey tool)*
  - parents / carers
  - staff

Context

The Isle of Ely Primary e-Safety Policy has been written by the school, building on the London Grid for Learning (LGfL) exemplar policy and Becta guidance. It has been designed to link with other relevant policies, such as the Child Protection, Behaviour and Anti-Bullying policies.

National guidance suggests that it is essential for schools to take a leading role in e-safety. DfE(Becta) in its 'Safeguarding Children in a Digital World' suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-school links and extended school activities, DfE recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to all learners. The benefits are perceived to "outweigh the risks." However, schools must, through their e-safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. This policy will also form part of the school's protection from legal challenge, relating to the use of ICT.

'Harnessing Technology: Transforming learning and children's services' [1] sets out the government plans for taking a strategic approach to the future development of ICT.

> *"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners.*
> *To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom."* DfE, eStrategy 2005

'Every Child Matters'[2] and the provisions of 'Working Together to Safeguard Children'[3] sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The 'staying safe' outcome includes aims that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

Much of these aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

[1] http://www.dfes.gov.uk/publications/e-strategy/

[2] See The Children Act 2004 [http://www.opsi.gov.uk/acts/acts2004/20040031.htm]

[3] Full title: Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children. See Every Child Matters website [http://www.everychildmatters.gov.uk/_files/AE53C8F9D7AEB1B23E403514A6C1B17D.pdf]

1. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- e-mail
- Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com)
- Video broadcasting sites (Popular: http://www.youtube.com/)
- Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
- Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/)
- Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down 'Office' applications.

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at Isle of Ely Primary School:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education programme for pupils, staff and parents

Reference: Becta - E-safety Developing whole-school policies to support effective practice [4]

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The headteacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior management team.

Our school **e-Safety Co-ordinator** is Bryony Surtees

Our e-Safety Coordinator ensures they keep up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP)[5]. The school's e-Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance [6] on e-Safety and are updated at least annually on policy developments.

[4] http://schools.becta.org.uk/index.php?section=is

[5] http://www.ceop.gov.uk/

[6] Safety and ICT - available from Becta, the Government agency at: http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_str_02&rid=10247

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools’ Policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs and use of website
- eBullying / Cyberbullying procedures
- Their role in providing e-Safety education for pupils

Staff are reminded / updated about e-Safety matters at least once a year.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/mentoring by member of the Senior Management Team/ Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
- referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or other camera devices				✓				✓
Use of hand held devices e.g. PDAs, PSPs				✓				✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs		✓						✓

When using communication technologies the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored.** *Staff and pupils should use only the school email service to communicate with others when in school, or on school systems*
- **Users need to be aware that email communications may be monitored**
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**
- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.*
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by LGfL and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational/non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce			✓			
File sharing					✓	
Use of social networking sites			✓			
Use of video broadcasting e.g. Youtube		✓				

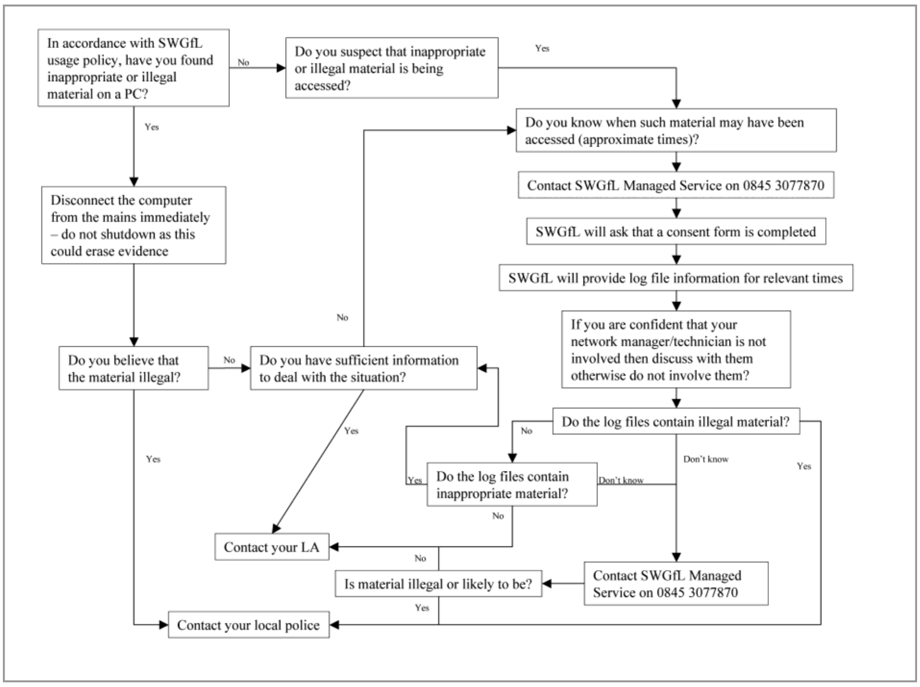
Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

The e-safety flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.


In accordance with SWGfL usage policy, have you found inappropriate or illegal material on a PC?
No
Do you suspect that inappropriate or illegal material is being accessed?
Yes
Yes
Do you know when such material may have been accessed (approximate times)?
Contact SWGfL Managed Service on 0845 3077870
SWGfL will ask that a consent form is completed
SWGfL will provide log file information for relevant times
Disconnect the computer from the mains immediately – do not shutdown as this could erase evidence
No
If you are confident that your network manager/technician is not involved then discuss with them otherwise do not involve them?
Do you believe that the material illegal?
No
Do you have sufficient information to deal with the situation?
Do the log files contain illegal material?
Yes
No
Don't know
Yes
Yes
Yes
Do the log files contain inappropriate material?
Don't know
No
Contact your LA
No
Is material illegal or likely to be?
Contact SWGfL Managed Service on 0845 3077870
Yes
Contact your local police

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the LGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Phase Leader/ICT Subject Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		✓	✓	✓		✓			
Unauthorised use of non-educational sites during lessons	✓	✓	✓			✓			
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓			✓			
Unauthorised use of social networking / instant messaging / personal email	✓	✓	✓			✓			
Unauthorised downloading or uploading of files	✓	✓	✓						
Allowing others to access school network by sharing username and passwords	✓	✓	✓			✓			
Attempting to access or accessing the school network, using another pupil's account	✓	✓	✓			✓			
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓			✓			
Corrupting or destroying the data of other users	✓	✓	✓			✓			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			✓	✓		✓			
Continued infringements of the above, following previous warnings or sanctions			✓			✓	✓		✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			✓			✓			✓
Using proxy sites or other means to subvert the school's filtering system			✓				✓		
Accidentally accessing offensive or pornographic material and failing to report the incident			✓			✓			
Deliberately accessing or trying to access offensive or pornographic material			✓				✓		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			✓				✓		

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓				✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓	✓					✓
Unauthorised downloading or uploading of files		✓	✓			✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓	✓					✓
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓				✓		
Deliberate actions to breach data protection or network security rules		✓	✓					✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓		✓			✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓	✓	✓				✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils		✓	✓	✓				✓
Actions which could compromise the staff member's professional standing		✓	✓					✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓					✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓					✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓	✓				✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓					✓
Breaching copyright or licensing regulations		✓	✓					✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓					✓