Ashton Keynes C of E Primary School
Internet and E-Safety Policy Internet and eSafety Policy

This policy has been written by the school, building on the SWGfL policy template and government guidance. It has been agreed by the senior management and approved by governors and FOAKS. The 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.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education, including all members of the school staff and governors, parents, representative members of the community e.g. Reverend Shirley, and the children themselves.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

It is the responsibility of all persons connected with the school to be vigilant in reporting any e-safety concerns to the e-Safety Leader (Sarah Igoe).

E-Safety throughout the school

E-Safety depends on effective practice at a number of levels:

- ★ Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- ★ Sound implementation of the e-safety policy in both administration and curriculum, including secure school network design and use.
- ★ Safe and secure broadband from the SWGfL including the effective management of Web filtering.
- ★ National Education Network standards and specifications.

eSafety Risks

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- ★ Access to illegal, harmful or inappropriate images or other content
- ★ Unauthorised access to / loss of / sharing of personal information
- ★ The sharing / distribution of personal images without an individual's consent or knowledge
- ★ Inappropriate communication / contact with others, including strangers
- ★ Cyber-bullying
- ★ Access to unsuitable video / internet games
- ★ An inability to evaluate the quality, accuracy and relevance of information on the internet
- ★ Plagiarism and copyright infringement
- ★ Illegal downloading of music or video files
- ★ The potential for excessive use that may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the real world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

eSafety Policy Summary

This Policy is available for staff on the school server and available for parents on the school website.

The Designated Child Protection Co-ordinators are: Samantha Saville, Daniel Hockaday, Anna O'Neill, Jade Smith and Sarah Igoe
The eSafety Leader is: Sarah Igoe
The school's managed service provider for computing is SOS Computing

All staff sign a Staff Computing Acceptable Use Policy on appointment and thereafter on an annual basis. School eSafety rules have been set for pupils and are on display around the school, this are also talked about during the start of every new academic year. Parents sign and return an agreement that their child will comply with the School eSafety rules when their child joins the school and annually thereafter at the start of the school year.

Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.

Personal data is collected, stored and used according to the principles of the Data Protection Act.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.
The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.
The school will deal with such incidents within this policy and associated behaviour policy and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. It is important for parents to inform the school if their child has been involved in any incident that the school may not be aware of. Children are not permitted to bring mobile phones or other electronic devices to school.

1. Writing and reviewing the e-safety policy

The eSafety Policy relates to other policies including those for Computing, behaviour and for child protection.

- ★ Our eSafety Policy has been written by the school, building on the SWGfL eSafety guidelines and government guidance.

2. Teaching and learning

2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Refer to appendix 1 – Teaching, Learning and the Internet

2.3 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and 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 in KS1 and KS2 will be taught about e-Safety each term following guidance from Wiltshire and government documentation. Pupils will be taught that the following are not permitted within school and the community; displaying offensive messages or pictures, using obscene language, harassing, insulting or attacking others (whether on or off school premises or within/outside of normal school hours), damaging computers, computer systems or computer networks, using others people's logons/passwords, trespassing in others' folders, work or files, intentionally wasting limited resources. Pupils are also taught the importance of not involving themselves in any of the above actions in or outside of school.

- The school will use the nationally recognised 'Think U Know' e-Safety material to support e-Safety teaching and learning within school.

- Pupils should be directed to specific websites checked by their teacher and use a child friendly safe search when possible e.g. www.swiggle.co.uk

2.4 e-Safety and portable equipment

This section covers all portable equipment whether owned by the school or by other persons and brought onto school grounds.

The school provides portable Computing equipment such as laptop computers, word processors, digital microscopes and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- ★ No portable equipment or devices will be used to harm or embarrass another person.
- ★ No portable equipment or devices will be used to bully or intimidate another person.
- ★ Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Staff Computing Acceptable Use policy.
- ★ All files leaving the school site should be encrypted and should only be accessible using a 'strong' password containing a combination of letters, numbers and keyboard symbols or placed onto a password protected memory stick that are provided by the school.

2.5 Managing Internet Access

2.5.1 Information System Security

- ★ School ICT systems capacity and security will be reviewed regularly by SOS Computing
- ★ Virus protection will be updated regularly by SOS Computing

2.5.2 E-mail and messaging

- ★ Pupils may only use approved e-mail accounts on the school system.
- ★ Pupils must immediately tell a teacher if they receive offensive e-mail.
- ★ Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- ★ E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- ★ The forwarding of chain letters is not permitted.
- ★ Message content should not cause offense or be likely to cause offense
- ★ Any incidents involving inappropriate use of e-mail should be dealt with by the class teacher in conjunction with the e-Safety Subject leader. Parents should be informed.
- ★ Pupils should be reminded to write polite, friendly non-offensive messages and emails

2.5.3 Published content on the school website

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

2.5.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully. Staff should consider using group photographs rather than full-face photos of individual children when possible. Any photographs selected must be used in line with the parent's wishes, stated on their child's Parental Permission form - see appendix 2.
- Pupils' full names will not be used anywhere on a school Website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school learning platform
- Work can only be published with the permission of the pupil and parents/carers.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic devices.

2.5.5 Social networking and personal publishing

- The school's internet provider, SWGfL, will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- 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 in and out of school
- If social networking platforms are used by teachers to support their class' learning such as a class blog, all postings and comments must be approved by the account administrator before being published.

2.5.6 Managing filtering

- The school will work with the LA, SWGfL and SOS Computing to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials the teacher or adult supervising them should report the incident to the e-Safety Leader who will follow through as required.

2.5.7 Internet use at home

- Parents and Carers will be advised to contact their own Internet Service Providers to explore home filtering and child controls.
- Parents are advised not allow their child unsupervised access to the internet, whether on computers or mobile devices.
- Parents should be advised to visit the Links section of the school website for further information on eSafety at home.

2.6 Managing videoconferencing

- Pupils will be supervised by a teacher when making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

2.7 Managing emerging technologies

- ★ Emerging technologies will be examined for educational benefit and an informal risk assessment will be carried out by the class teacher before use in school is allowed.
- ★ All staff members should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- ★ Pupils are not permitted to bring mobile phones or other electronic devices into school.
- ★ Staff will use the school phone system where contact with pupils or parents is required unless working off site or on school visits. In the first instance, the school office should be contacted to make contact with the pupil or parent. Mobile phones should only be used as a last resort.

2.8 Protecting personal data & Data Transfer

- ★ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- ★ Staff are responsible for keeping sensitive pupil data secure when taken off the school site.
- ★ Encrypted USB memory sticks should be used to transfer files between home and school.

3 Policy Decisions

3.1 Authorising Internet access

- ★ All staff must read and sign the Staff ICT Acceptable Use Policy on appointment and annually thereafter before using any school ICT resource.
- ★ Access to the Internet will be by adult demonstration with occasional directly supervised access to on-line materials.
- ★ Parents will be asked to sign and return a consent form for use of the internet in school – see Appendix 2
- ★ The school will maintain a current record of all staff and pupils who are granted access to school computing systems.

3.2 Assessing risks

- ★ The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SWGfL can accept liability for the material accessed, or any consequences of Internet access.
- ★ The school will audit computing provision to establish if the e-safety policy is adequate and that its implementation is effective. Any required changes will be communicated with SOS Computing.

3.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with initially by the e-Safety Leader (Sarah Igoe). See Appendix 3 – SWGfL E-Safety Incident Flow Chart.
- When incidents are reported to the eSafety leader, a report will be filed and records kept.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Complaints of a bullying nature must be dealt with in accordance with the school behaviour policy and procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- When handling complaints about the way the school has dealt with an e-Safety incident, all complaints will be dealt with in accordance to the school complaint procedure/policy.

4. Communications Policy

4.1 Introducing the e-safety policy to pupils

- e-Safety rules will be available in all rooms where computers are used and discussed with pupils regularly. See appendix 4 – E-Safety Rules
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up
- e-Safety training will be embedded within the computing scheme of work and the Personal Social and Health Education (PSHE) curriculum.

4.2 Staff and the e-Safety policy

- All staff will be given the School *e-Safety Policy* and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff are required to sign the Staff ICT Acceptable Use policy
- Breaches of the Staff ICT Acceptable Use policy will be dealt with in accordance to the flow chart in appendix 1.
- CPD meetings will be arranged to raise the awareness of e-Safety.
- New staff, as part of their induction pack, will be given an up-to-date copy of the e-Safety policy.

4.3 Enlisting parents' support

- Parents and carers' attention will be drawn to the School e-Safety policy via the school website.
- The school will maintain a list of e-safety resources for parents/carers on the Links page of the school website.
- The school will ask all new parents to update and sign a Parental Permission Form for Internet Access, Children's Image Use and Web Publication when they register their child with the school and annually at the start of each academic year.

4.4 Community use of the Internet

- The school will provide guest access to wireless internet for community users.

Pupil Voice

Acceptable Use Policy for learners in KS1

I want to feel safe all the time.

I agree that I will:

- ★ always keep my passwords a secret
- ★ only open pages which my teacher has said are OK
- ★ only work with people I know in real life
- ★ tell my teacher if anything makes me feel scared or uncomfortable on the internet
- ★ make sure all messages I send are polite
- ★ show my teacher if I get a nasty message
- ★ not reply to any nasty message or anything which makes me feel uncomfortable
- ★ not give my mobile phone number to anyone who is not a friend in real life
- ★ only email people I know or if my teacher agrees o only use my school email
- ★ talk to my teacher before using anything on the internet
- ★ not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- ★ not upload photographs of myself without asking a teacher
- ★ never agree to meet a stranger

Acceptable Use Policy for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- ★ always keep my passwords a secret
- ★ only use, move and share personal data securely
- ★ only visit sites which are appropriate
- ★ work in collaboration only with people my school has approved and will deny access to others
- ★ respect the school network security
- ★ make sure all messages I send are respectful
- ★ show a responsible adult any content that makes me feel unsafe or uncomfortable
- ★ not reply to any nasty message or anything which makes me feel uncomfortable
- ★ not use my own mobile device in school unless I am given permission o only give my mobile phone number to friends I know in real life and trust
- ★ only email people I know or approved by my school
- ★ only use email which has been provided by school
- ★ obtain permission from a teacher before I order online
- ★ discuss and agree my use of a social networking site with a responsible adult before joining
- ★ always follow the terms and conditions when using a site
- ★ always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- ★ always check with a responsible adult before I share images of myself or others
- ★ only create and share content that is legal
- ★ never meet an online friend without taking a responsible adult that I know with me

Appendix 1 – Teaching, Learning and the Internet

Possible T & L activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on moderated sites and by the school administrator.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.

Appendix 2 – Parental Permissions form

Parental Permissions

Please complete, sign and return to the class teacher

Pupil: *……..……..…….* ***Class:*** *……*

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and follow these rules at all times.

Signed (by the child): *…….….……* ***Date:*** *…….*

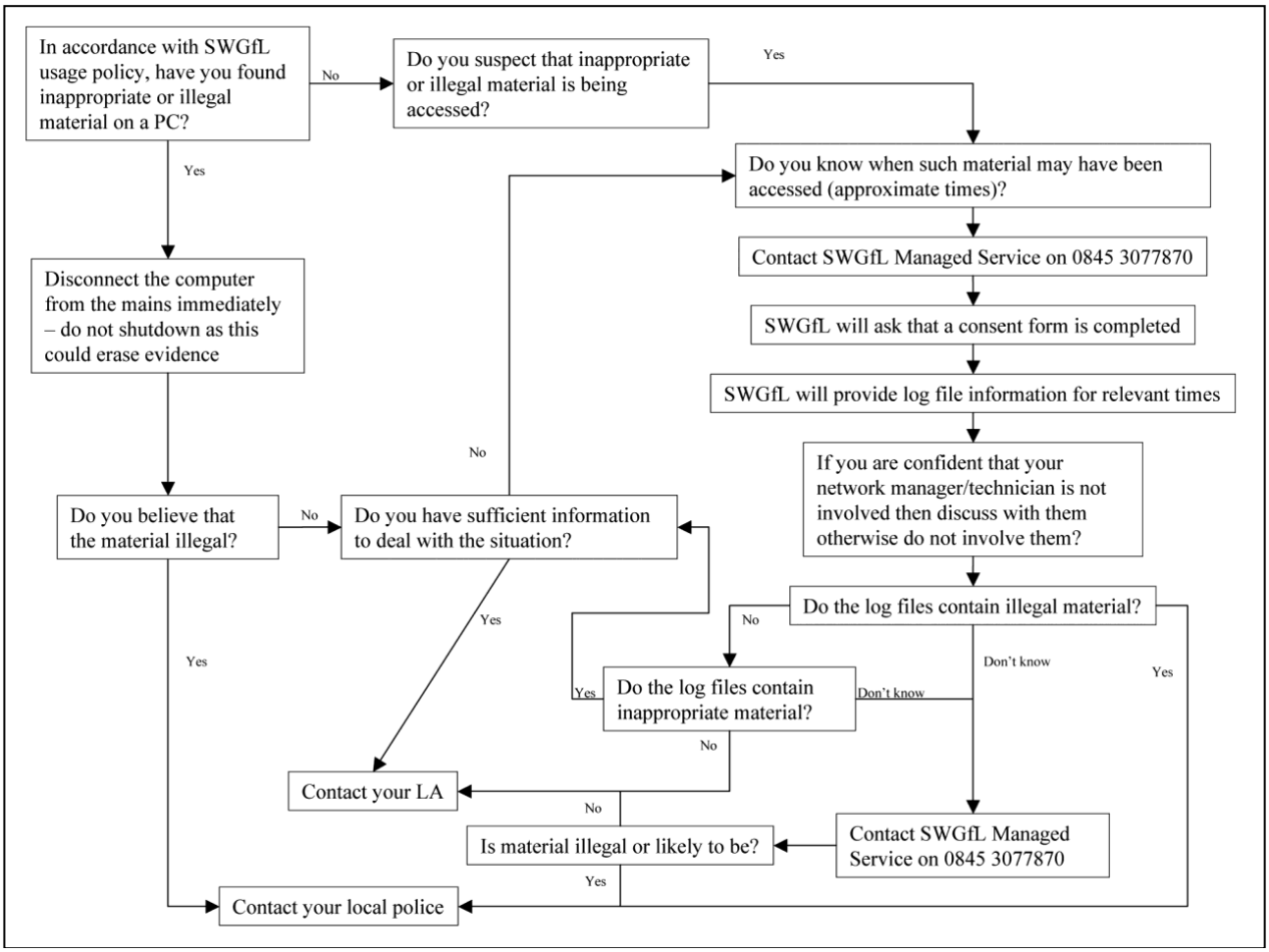
Parent's Consent	**Tick if you give permission**	**Tick if you DO NOT give permission**
I have read and understood the school rules for responsible Internet use and give permission for my child to access the **Internet**.		
Photos or examples of my **child's work** (including images and sound files) may be published on the school **website**.		
Photos of **my child** may be used for school publicity and be released to the **media**.		
Photos of **my child** may be published on the school **website**.		
Videos of **my child** may be published on the school **website**.		
Photos of **my child** may be used **within** the school, in their work and on display.		
My child can take part in supervised visits around the village.		

Signed: *…….……..……* ***Date:*** *…….*

Please print name:

…….……..……

Appendix 3 – SWGfL eSafety Incident Flow Chart



Ashton Keynes C of E Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- I will ask permission before using the Internet.
- I will only use the Internet when a member of staff is present.
- I will use only my class network login and password, which is secret.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give my home address or phone number, or arrange to meet someone.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The South West Grid for Learning (SWGfL) monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.