Carbeile Junior School
E-Safety Policy

VM – July 2017

1. Background / Rationale

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 from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student 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 risk of being subject to grooming by those with whom they make contact on the internet.
- 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 which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg 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 pupils' 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.
Our e-safety policy explains how we safeguard against these risks, 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.

1. Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by an e-safety committee made up of:

- School E-Safety Coordinator: Mrs. V. Marks
- Headteacher: Mr P Hamlyn
- Dedicated Safeguarding Lead (DSL): Mr P Hamlyn & Mrs J Evans
- Deputy Head: Miss C Rendall
- Governor: Mr D Marsh
- SENDCO: Mrs J Evans

Consultation with the whole school community will take place through the following:

- Staff meetings
- School Council
- INSET Day
- Governors meeting / sub committee meeting
- Digital Leader meetings
- School website / newsletters

2. Schedule for Development / Monitoring / Review

This e-safety policy was reviewed by the Governing Body / Governors Sub Committee on:	*Reviewed 09.07.17*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Committee & Governors*
This policy will be reviewed:	*July 2019*

The school will monitor the impact of the policy using:

- Logs of reported incidents (E-Safety Log of Incidents form kept by Mr. Hamlyn and the e-safety lead)
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity (via server)
- Year surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

3. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school Computing 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 and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

a. Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role will include:

- regular meetings with the E-Safety Co-ordinator.
- regular monitoring of e-safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors committee / meeting

b. Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher & SLT are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular reports from the E-Safety Co-ordinator.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

c. E-Safety Coordinator (assisted by Child Protection Officers):

- leads the Digital Leaders
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school Computing technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments. (see e-safety log – kept in the e-safety folder in the office/ blank log forms kept in the office)
- meets with E-Safety Governor to discuss current issues, review incident logs and filtering.
- attends relevant meeting / committee of Governors
- reports regularly to SLT.

d. Network Manager / Technical staff:

The Computing Co-ordinator/ external support agency(IT and Network Services)

- that the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid

- the school's applies the filtering policy of the SWgFl and will make no change to what can be filtered, it is updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network and email is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator / DSL / SLT for investigation, action and sanction .
- monitoring software systems are implemented and updated.

e. Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem (following the E-safety incident log process) to the E-Safety Co-ordinator, child protection offer, senior management team for investigation, action or sanction
- digital communications with pupils (email / voice) should be on a professional level and only carried out using official school systems.
- e-safety issues are embedded in the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor Computing activity in lessons, extra-curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- they follow the Switched onto Computing curriculum and teach E-safety as part of each lesson

f. The Child Protection Officer

Is trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

g. Students / pupils:

- are responsible for using the school Computing systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

h. Parents / Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evening/workshops, newsletters, letters, website and information about e-safety literature and campaigns.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website and in future pupil records in accordance with the relevant school Acceptable Use Policy.

i. Community Users

Community Users who access school Computing systems / website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.)

5. Policy Statements

i. Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorials.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

ii. Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the SWGfL Safe website (the SWgFl "Golden Rules" for parents)

iii. Education - Extended Schools

The school will offer family learning courses in Computing, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

iv. Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-safety Policy and Acceptable Use Policies.
- The E-Safety Coordinator will receive regular updates through attendance at SWGfL / LA training sessions and by reviewing guidance documents released by BECTA / SWGfL / LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice, guidance and training as required.

6. Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in Computing / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.
- Participation in school training / information sessions for staff or parents

7. Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School computing systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school computing systems
- Servers, wireless systems and cabling must be securely located and physical access restrComputinged
- All users will have clearly defined access rights to school computing systems.*).*
- All users will be provided with a username and password by the Computing coordinator who will keep an up to date record of users and their usernames.
- The “master / administrator” passwords for the school computing system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader (E-Safety Coordinator) and kept in a secure place (e-safety folder in office).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by SWGfL
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the head teacher and e-safety co-ordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by the Network Manager to control workstations and view users activity

- An appropriate system is in place for users to report any actual / potential e-safety incident to the e-safety/ computing coordinator (E-safety Log Forms – kept in the office/ or report directly to e-safety/ computing-co-ordinator/ SLT, who will keep an e-safety incident report form , kept in the (e-safety)folder.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system.
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from installing programmes on school computers.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices.
- The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data can not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

8. Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of computing across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students / pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes and **must** be deleted before equipment is taken off school property.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil’s work can only be published with the permission of the pupil and parents or carers.

9. 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 or 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

v. 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 :

	Staff & other adults				Students / 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	*						*1	
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 eg 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				*				*

*1 Pupils phones to be handed in to each teacher in the morning and only returned in the afternoon.

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 students / pupils should therefore 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 students / pupils or parents / carers (email, chat 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 students / pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Students / 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.

vi. Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restrComputings 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,	**child sexual abuse images**					*
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					*

communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**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 SWGfL 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 (eg 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)					*	
On-line gaming (non educational)					*	
On-line gambling					*	
On-line shopping / commerce				*		
File sharing				*		
Use of social networking sites					*	
Use of video broadcasting eg Youtube				*		

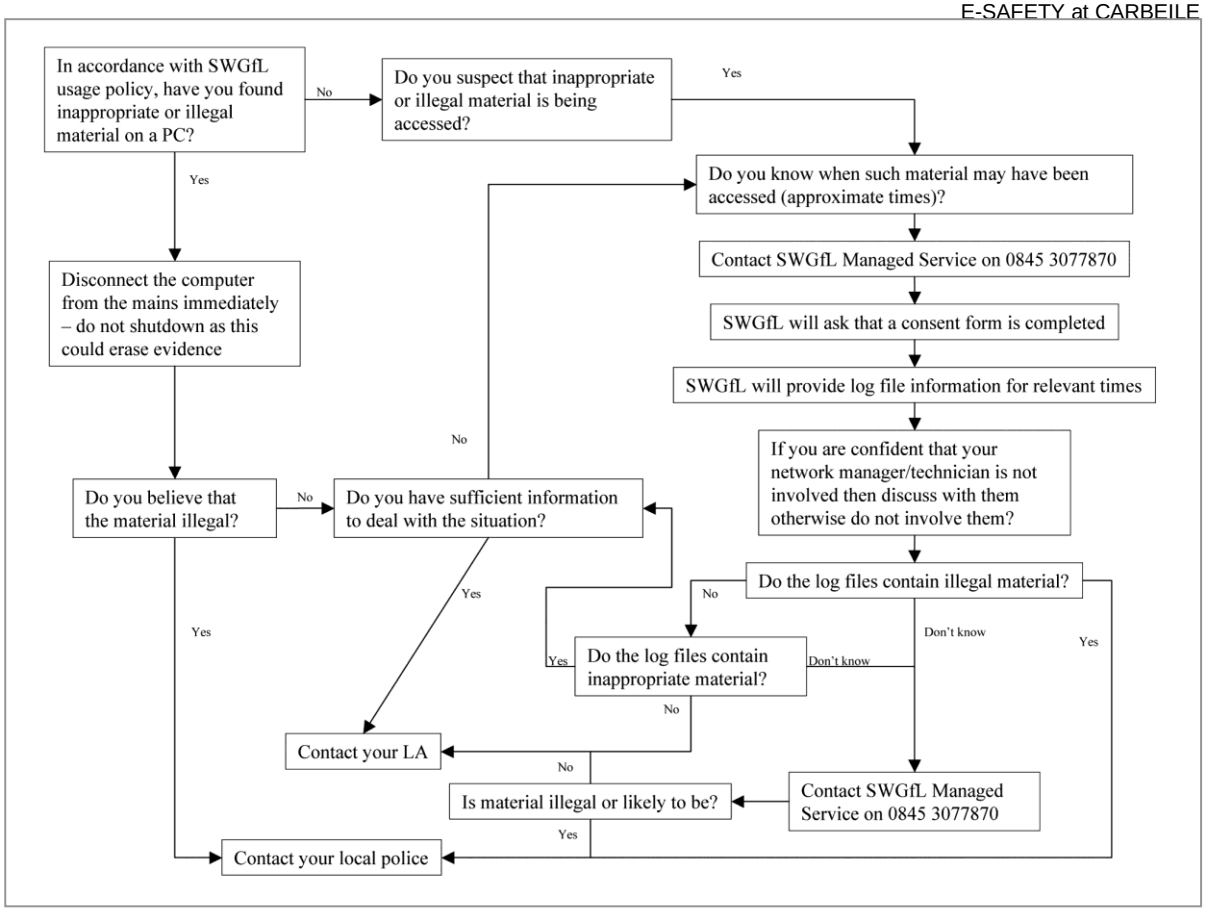
vii. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of COMPUTING, 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 SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp 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.



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 SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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:

Actions / Sanctions

Students / Pupils

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	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 eg 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 student's / 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 managerr	Refer to Headteacher	RRefer 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 eg 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 students / 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	*	*	*	*	*	*	*	*

viii. Related Documents

Carbeile Junior School E-Safety

Computing Policy
SWGfLT (South West Grid for Learning Trust) School E-Safety Policy
Safeguarding & Child Protection Policy
Health & Safety
Carbeile Junior School Staff & Volunteer Acceptable Use Policy Agreement
Carbeile Junior School Acceptable Use of the Internet for Pupils and Safety Rules
SMART Rules
E-Safety Incident Log
E-safety incident log process

ix. Practical Outcomes:

1. E-safety folder held by lead (e-safety policies and incident log forms)
2. E-sfatey Log Forms – with Computing lead and Mr. Hamlyn
3. All users to sign an internet AUP.
4. SMART rules displayed in every classroom.
5. On-going monitoring of e-safety.
6. An age appropriate e-safety activity to be planned for each year group, once per term.
7. An E-safety assembly.
8. Digital leaders to be responsible for classroom management of equipment and meeting with e-safety lead to plan activities and learning opportunities.

x. Acknowledgements

Date on which policy was approved in July 2010

Reviewed: July 2011 – Practical outcomes 8 and 9 added.

Reviewed: Spring 2012 – Overview document produced for school website.

Reviewed: January 2013 – No changes except Governor responsibility.

Reviewed: January 2014 – Changes to individual responsibilities, removal of names from main content and restrictions on use of YouTube.

Reviewed: June 2015 – Changes to individual responsibilities & job titles, removal of reference to ICT and replaced ICT with ‘computing’, removal of references to VLE.

Reviewed: July 2017 – Changes made to reflect changes in the curriculum and changes in equipment used by the school. Teachers are permitted to take photos using their school iPads, but these must be deleted **before** they are taken away from school property. Teachers must use secured devices to store personal information about pupils, which should be password encrypted. E-safety incident logging must now be reported following a flow diagram; this should be understood and displayed by each teacher. E-safety must be taught in every lesson, as part of the new Computing curriculum.

Date: 11th July 2017

Headteacher: Mr. P. Hamlyn

Chair of Governors: Mrs. S. Morton

Co-ordinator: Mrs. V. Marks

Review Date: July 2019