Bidford on Avon C. of E Primary School.

E-Safety Policy

September 2015

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by the following stakeholders using a template from the SWGFL:

- Headteacher / Senior Leaders
- E-Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Children and the School Council
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Monitoring and Review

This e-safety policy was approved by the Governing Body on:	Insert date
The implementation of this e-safety policy will be monitored by the:	Senior Leadership Team, e-safety coordinator, Governors, school council.
Monitoring will take place at regular intervals:	Yearly
The Governing Body 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:	Governor meetings
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:	September 2016
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police – where advised

The school will monitor the impact of the policy using:

- Logs of reported incidents
- LA monitoring of internet use
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

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 the school. It sets out how we strive to keep pupil safe with technology in school and educate children and support parents/ carers about the potential risks here, at home and in the wider community.

The potential that technology has to impact on the lives of all citizens, including children increases on year. In many areas technology is transforming the way that schools teach and children learn. At home technology is changing the way children live and the activities in which they choose to partake. While developing technology brings many opportunities, it also brings risks and potential dangers to children and staff of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to personal information or private data
- Grooming by those with whom they make internet contact
- Unauthorised sharing/ distribution of personal images
- Inappropariate communication with others
- Cyber bullying
- Acces to unsuitable videos and games
- Copyright infringement
- Illegal downloading
- Data handling

This policy sets out how we strive to keep pupil safe with technology in school and educate children and support parents/ carers about the potential risks here, at home and in the wider community

.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students 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 outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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.

Roles and Responsibilities

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

Responsibilities of 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 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 combined with that of the Child Protection / Safeguarding Governor). The role of the E-Safety Governor will include:

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

Responsibilities of the Headteacher and Senior Leaders:

- The Headteacher has a duty of care 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, Assistant Headteacher and members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents
- The Headteacher Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring termly reports from the E-Safety Co-ordinator / Officer.

Responsibilities of the E-Safety Coordinator:

The Headteacher, Mr Simms and Assistant headteacher, Mrs Whiting, has day to day responsibility for e-safety:

- leads the e-safety committee and meets on a regular basis
- 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 the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets termly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

Responsibilities of Local Authority Technical staff:

The Headteacher, bursar and the Local Authority Technical//Computing department is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed by local authority
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep 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 / internet / portal / email is regularly monitored, by local authority, in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Coordinator for investigation / action / sanction. A report, generated by the local authority, is sent to the Headteacher monthly
- that monitoring software / systems are implemented and updated as agreed in school / academy policies

Responsibilities of 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 Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Headteacher/ E-Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- all classroom pcs , laptops and mobile technology should be secured at times when the classroom is empty, by locking the computer
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies, which have developed with the children's involvement, through the school council
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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

Responsibilities of Child Protection / Safeguarding Designated Person

is trained in e-safety issues and aware of the potential for serious child protection / safeguarding 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

Responsibilities of School council:

- Develop e-safety awareness throughout the school.
- To discuss issues relating to e-safety, with the support of the e safety coordinator/ governor and staff. Issues that arise are referred to other school bodies as appropriate and when necessary to outside bodies such as the Safeguarding children board. Parents are also consulted on provision for e-safety and its impact.
- Issues may arise through participating in the Peer Mediation scheme, discussion with Young Leaders, discussion with teaching staff and other trusted adults and through 'Worry Boxes' in each classroom.

Responsibilities of Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Safe internet use rules
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand 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

Responsibilities of Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, attending e-safety assemblies, and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to the school website and portal

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- pupils are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Pupils know what to do if the encounter inappropariate material e.g turnoff the monitor or turn the ipad over, report the incident to an adult.

Acceptable use agreements:

All members of the school community are responsible for using ICT systems in accordance with the appropriate acceptable use agreement, which they will be expected to sign before being given access to the school systems

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils/parents
- Staff and volunteers

Acceptable use agreements are introduced at parent induction meetings and signed by parents (KS1) and pupils (KS2) as they enter the school or Key Stage.

All employees of the school and volunteers sign when they take up their role in school at any stage during the year.

Acceptable use is supported by 'Acceptable Use' posters displayed in classrooms and working areas, including the ICT suite.

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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to consult with and provide information and awareness to parents and carers through:

- Curriculum activities/ consultation
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

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. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- More immediate training/discussion in light of emerging new technologies/e-safety issues, delivered to staff in staff meetings or other inset occasions.
- 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 Agreements.
- The E-Safety Coordinator, Mr Thackway, and Headteacher, Mr Simms, will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

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 technology / 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 / or other relevant organisation.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

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 technical systems will be managed in ways that ensure that the school meets the technical requirements recommended by the Local Authority and other relevant guidance.
- There will be annual reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password from Year 2 onwards. Users are responsible for the security of their username and password. Class log-ons and/or usernames are used in Reception and Year 1.
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher, bursar or other nominated senior leader and kept in a secure place

- The bursar is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- The Local Authority monitors and records the activity of users on the school technical systems – reporting any inappropriate use to the headteacher and users are made aware of this in the Acceptable Use Agreement
- Any actual or potential technical incident / security breach should be reported to the ICT subject leader, Mr Thackway, and to the e-safety coordinator, Mrs Whiting or Mr Simms.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Trainee teachers, supply teachers, visitors are provided with 'guest' accounts to access the school systems following induction on e-safety.
- Staff must ensure that when using school devices at home that they restrict their use to school business and the use of work email accounts. Family members must not be permitted to use school devices.
- Downloading executable files and installing programmes on to the school curriculum network is only permitted with the permission of the headteacher. Downloading apps onto school devices can be done by staff only with the permission of the headteacher in consultation with the safety coordinator.
- All removable media (eg memory sticks / CDs / DVDs) must use passwords/ encryption – CD/DVDs must not be used to store data, information or images. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured- using the Local Authority portal.

Use of digital and video images

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, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. 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.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers 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.
- 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

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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO), Mr Simms
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software. Stone laptops are installed with anti-virus 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:

Communication Technologies	Staff & other adults				Students / Pupils			
	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 / cameras		✓					✓	
Use of other mobile devices eg tablets, gaming devices	✓						✓	
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓			✓	
Use of messaging apps				✓				✓
Use of social media		✓					✓	
Use of educational blogs		✓					✓	

E-mail

Access to email is provided for all users in school via the Warwickshire Welearn365 gateway and portal 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. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff, students and parents/ carers should only take place within the context of curriculum work (portal email system/ blogging) and must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may 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 e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Website and the Learning Platform

Our school uses the public facing website for sharing information with the community beyond our school. This includes celebrating work and achievements of children

- Personal information will not be posted on the school website and only official email addresses used to identify members of staff.
- Only pupils first names will be used
- Detailed calendars will not be published
- Photographs published on the website will be carefully selected and will comply with the following good practice guidance on the use of images
    - pupils' full names will not be used and never in association with photographs
    - photographs will not provide any identifying details
    - written permission from parents or carers will be obtained before images are published on the website

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school / academy* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers/ staff or school business
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information and access to personal messages/ images is not accessible to the general public.
- In respect of teachers' professional conduct as set out in 'Teachers Standards, staff should not engage in any online activity that may bring themselves, the school or the profession into disrepute. Staff need to be aware of the language and tone of messages used in public online spaces and of the appropriateness of images available for public viewing

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

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 usage as follows:

User Actions		Acceptable	Acceptable at certain	Acceptable for nominated	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 –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)				X		
On-line gambling					X	
On-line shopping / commerce				X		
File sharing			X			
Use of social media				X		

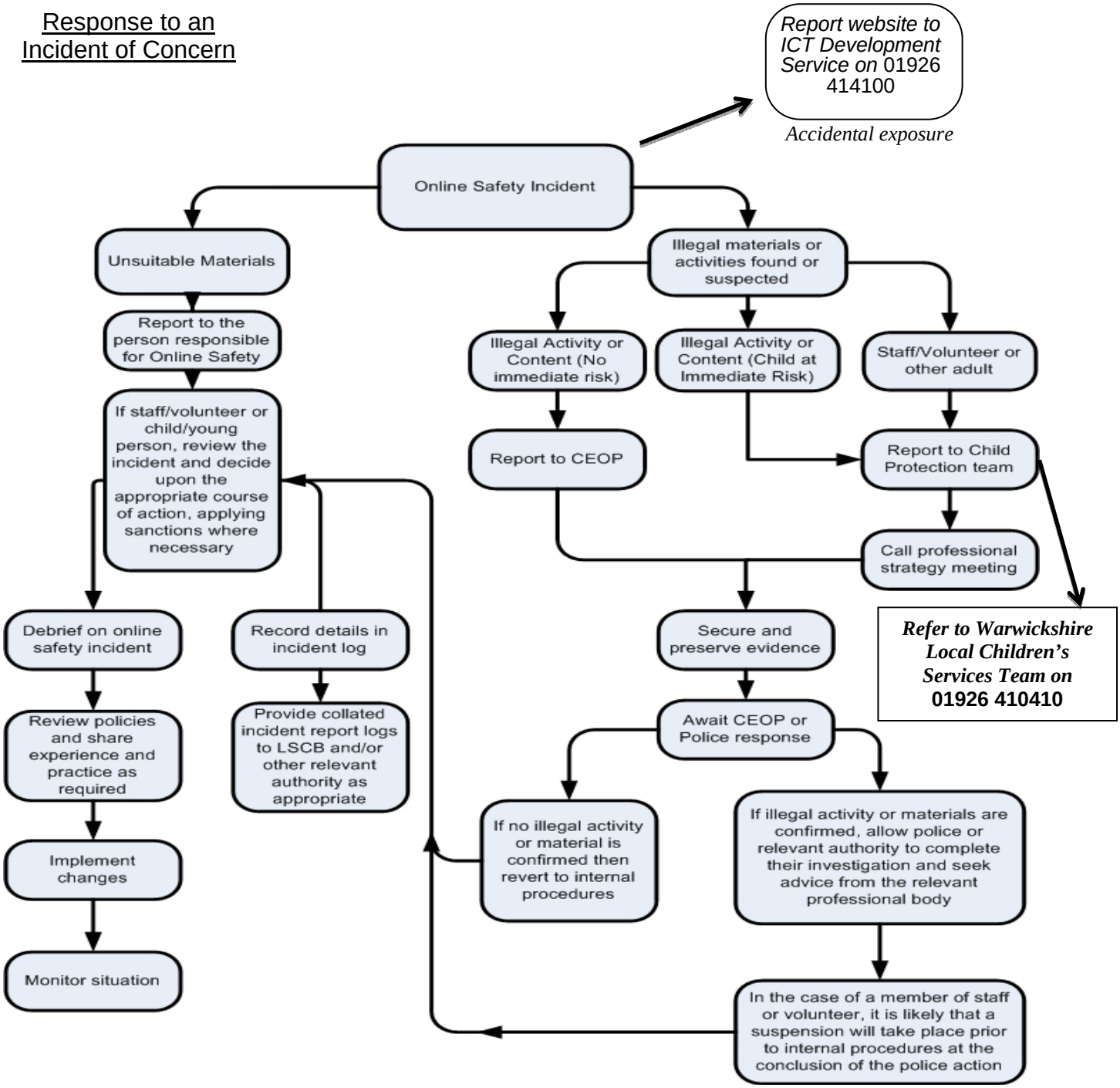
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities or accidental access to inappropriate material (see "User Actions" above). Staff and pupils need to feel comfortable to report incidents immediately and understand clearly the reporting procedures. All incidents should be recorded on the safety reporting form and presented to the headteacher or assistant headteacher.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

Staff and pupils need to feel comfortable to report immediately accidental access to inappropriate material. It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
- All incidents should be recorded on the safety reporting form and presented to the headteacher or assistant headteacher.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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:

Students / Pupils Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to safety coordinator	Refer to Headteacher / Principal	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).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X	X						X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	X
Unauthorised use of social media / messaging apps / personal email	X	X				X		X	
Unauthorised downloading or uploading of files	X	X						X	
Allowing others to access school network by sharing username and passwords								X	
Attempting to access or accessing the school network, using another pupil's account	X	X	X						X
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X			X
Corrupting or destroying the data of other users	X	X	X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X			X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X				X		

Staff Actions / Sanctions

Incidents:	Refer to line managerr	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering	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).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X	X						
Unauthorised downloading or uploading of files		X				X		
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	X	X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X	X	X			X		
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X				X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X			X		
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X				X		
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X
Breaching copyright or licensing regulations		X				X		
Continued infringements of the above, following previous warnings or sanctions		X	X		X			X

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Bidford on Avon C. of E. Primary School E-safety incident report

Date/time	
Report compiled by	
Nature of incident:	
Who was involved: pupil; staff; parent	
Where did it happen: home; school – classroom/ICT suite/corridor/shared area/playground/hall.	
Device used: computer; laptop; ipad.	
Action taken:	
A copy of this report should be handed to the headteacher or assistant headteacher.	

Bidford on Avon C. of E. Primary SchoolStaff (and Volunteer) Acceptable Use Policy Agreement

Staff / Volunteer Name

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, ipads email, portal etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / portal) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. Staff should not use their personal email addresses / mobile phones / social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school :

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement/ school e safety policy/ mobile device guidelines, in the same way as if I was using school

equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School /LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school :

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that in my personal use of the internet and social media any images or messages available to public view must demonstrate the high standards of personal and professional conduct set out in the Teachers' Standards.
- I understand that in my personal use of the internet and social media school information and issues should not be openly discussed.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Dear Parents

Use of the Internet in School

As part of the school's ICT programme we offer pupils supervised access to the Internet and e-mail. Access to the Internet enables pupils to explore website information while exchanging messages with other learners and teachers throughout the world.

We have a detailed E-Safety Policy, which is intended to help us make the most of the opportunities that the Internet offers, whilst minimising the possible risks. It includes a set of 'Rules for E-Safety' that staff will use and teach to the children - a copy is attached for your information.

Our Internet provider operates a filtering system that restricts access to inappropriate materials. Some pupils may find ways to access material that is inaccurate, illegal or offensive to some people. The school cannot be held responsible for the nature or content of materials accessed through the Internet and will not be liable under any circumstances for any damages arising from your child's use of Internet facilities.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, families will wish to be aware that some pupils may find ways to access material that is inaccurate or offensive to some people. However, we believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. During school, teachers will guide pupils toward appropriate materials and follow our agreed E-Safety rules.

Please sign the attached form confirming that you have received this letter and a copy of the E-Safety rules. You child also need to sign confirming that they have read and understood the E-Safety rules.

Should you wish to discuss any aspect of Internet use, please telephone to arrange an appointment with me.

Please complete the enclosed form and return to school.

Yours sincerely

Mr A Simms

Bidford on Avon Church of England Primary School

Rules for E-Safety

We use the school computers and internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- **We only use the internet under adult supervision.**
- **We only use websites our teacher has chosen.**
- **We only search the internet with permission from a member of staff using agreed search facilities and words.**
- **We do not download anything from the internet without staff permission.**
- **We do not fill in online forms or click on popup acceptance buttons.**
- **We only e-mail pupils our teacher has approved.**
- **We send e-mails that are polite and sensible.**
- **We do not give out personal information or passwords.**
- **We do not arrange to meet anyone.**
- **We do not open e-mails sent by someone we do not know.**
- **We do not use internet chatrooms or social network sites.**
- **We tell staff if we see anything we are unhappy with or if we receive messages we do not like.**
- **We know our school may check our computer files and monitor the internet sites we visit.**
- **We understand that if we deliberately break these rules, we could be stopped from using the internet or computers.**

Use of the Internet in School

Child's Name: _____

I confirm I have received the 'Use of Internet in School' letter and a copy of the E-Safety Rules.

Parent Signature: _____ Date: _____

As a school user of the internet, I agree to comply with school rules on its use. I will use the internet in a responsible way and follow all the rules explained to me by the school.

Pupil Signature: _____ Date: _____