St Nicholas
C of E Primary School

# E-Safety Policy

**E-safety Co-ordinator: Anita Hartley**
**Headteacher: Adam Walsh**
**E-safety Governor: Caroline Harris**

**Adopted: December 2016** **Revised: December 2017**

## 1. 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 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 and/or 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 (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build 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.

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

## 2. SCHEDULE FOR DEVELOPMENT/MONITORING/REVIEW

| | |
|---|---|
| This E-safety policy was approved by the Full Governing Body on: | 12th December 2016 |
| The implementation of this e-safety policy will be monitored by the: | Headteacher/SLT<br>E-Safety Co-ordinator<br>Governors |
| Monitoring will take place at regular intervals: | Autumn Term Annually |
| The Governing Body  will receive a report on the implementation of the e-safety policy including anonymous details of e-safety incidents at regular intervals: | Autumn 2 Governors Meeting |
| 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: | November 2017 |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | ICT Development Service, Warwickshire Police |

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity
- Internal monitoring data for network activity
- Surveys and questionnaires of pupils, parents and staff.

## 3. 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 each 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 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.

Each 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 e-safety roles and responsibilities of individuals and groups within the school.

### 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. The role of the E-Safety Governor / Director will include:

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

### HEADTEACHER AND DEPUTY HEADTEACHER

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 and Deputy Headteacher 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 flow chart on dealing with e-safety incidents).

The Headteacher is responsible for ensuring that the E-Safety Co-ordinator 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 Headteacher and Deputy 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 Headteacher and Deputy Headteacher will receive regular monitoring reports from the E-Safety Co-ordinator.

## E-SAFETY CO-ORDINATOR

The school will have a named member of staff with a day to day responsibility for e-safety, who:

- 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 / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors when required
- reports regularly to Headteacher and Deputy Headteacher

Investigation into incidents will be dealt with by the E-Safety Co-ordinator, with sanctions being the responsibility of the Headteacher or Deputy Headteacher in accordance with the Behaviour Policy.

## NETWORK MANAGER/TECHNICAL STAFF

The School has a managed ICT service provided by Warwickshire ICT Development Service. It is the responsibility of each school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the School’s e-safety policy and procedures.

Technical Staff in school, Computing Co-ordinator and Warwickshire ICTDS are responsible for ensuring:

- that each school’s technical infrastructure is secure and is not open to misuse or malicious attack
- that each school meets required e-safety technical requirements and any Local Authority 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
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix “Technical Security Policy Template” for good practice)
- 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, Welearn365, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or designated person for children protection for investigation, possible action and sanction
- that monitoring software and systems are implemented and updated as agreed in

school policies

## TEACHING AND NON-TEACHING STAFF

Teaching and non-teaching 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 or designated person for child protection for investigation, possible action and sanction
- all digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- 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
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 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

## CHILD PROTECTION DESIGNATED PERSONS

The designated persons for Child Protection at each school should be trained in e-safety issues and be 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

## PUPILS

- **are responsible for using their school's digital technology systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and the 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

### 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. Each school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Welearn365 and information about local and national e-safety campaigns and 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 parents' sections of Welearn365
- their children's personal devices in the school (where this is allowed)

### COMMUNITY USERS

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

## 5. 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 each school's e-safety provision. Children need the help and support of their 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 should be provided as part of Computing and PHSEE lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be 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 children visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, medicines, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can

temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be audit-able, with clear reasons for the need.

## EDUCATION - PARENTS AND 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 and regulation of the children's on-line behaviours. Parents may underestimate how often children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The School will seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, Welearn365
- Parents /information evenings and workshops
- High profile events and campaigns e.g. Safer Internet Day, Anti-Bullying Week.
- Reference to relevant websites and publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

## EDUCATION - THE WIDER COMMUNITY

The School will provide opportunities for local community groups to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- Each school's website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, voluntary organisations to enhance their e-safety provision.

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.

## EDUCATION AND 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. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- 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 Co-ordinator 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 and INSET days.
- The E-Safety Co-ordinator will provide advice, guidance and training to individuals as required.

## TRAINING - GOVERNORS

Governors should take part in e-safety training and awareness sessions, with particular importance for those who are members of the PPC subcommittee. 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, including assemblies and lessons.

## TECHNICAL - INFRASTRUCTURE AND EQUIPMENT, FILTERING AND MONITORING

**The School will be responsible for ensuring that the school network and Welearn365 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 ICT systems will be managed in ways that ensure that each school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of each school's 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 ICT systems and devices.
- All users will be provided with a username and secure password by ICTDS who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password when prompted in accordance with LA password policy.
- Staff teaching younger children may choose to use group or class log-ons and passwords but need to be aware of the associated risks.
- The network manager and administrator passwords for each school's ICT system must also be available to the Headteacher and kept in a secure place
- The Headteacher 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)
- The school maintains and supports the managed filtering service by Warwickshire ICTDS.
- Any filtering issues should be reported immediately to ICTDS via the Computing Co-ordinator or the Headteacher.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users - staff/pupils etc).
- Requests from staff for sites to be removed from the filtered list will be considered by SLT. If the request is agreed, this action will be made via email and recorded. Logs of such actions shall be reviewed regularly by the E-Safety group.
- Each school's technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the Computing Co-ordinator or Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls,

routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- The school infrastructure and individual workstations are protected by up to date anti-virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to download executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## CURRICULUM

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

- 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, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICTDS can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be audit-able, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- 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

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 cyber-bullying 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 e.g. 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 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 or 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
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## 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, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks and other mobile devices cannot be password protected)

- the device must offer approved anti-virus and malware checking software
- the data must be securely deleted from the device, in line with school policy 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 | | | | 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 blogs | | ✓ | | | | ✓ | | |

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

- **The official Welearn365 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 Welearn365 email service to communicate with others when in school, or on school systems (e.g. by remote access).
- **Users need to be aware that email communications may be monitored.**
- **Users must immediately report, to the nominated person - in accordance with the School's 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 and pupils or parents/carers must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Whole class/group email addresses may be used in the Early Years and KS1, while pupils at KS2 and above will be provided with individual Welearn365 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.

## SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, 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 pupils, parents/carers or school staff
- 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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 OR INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those 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:

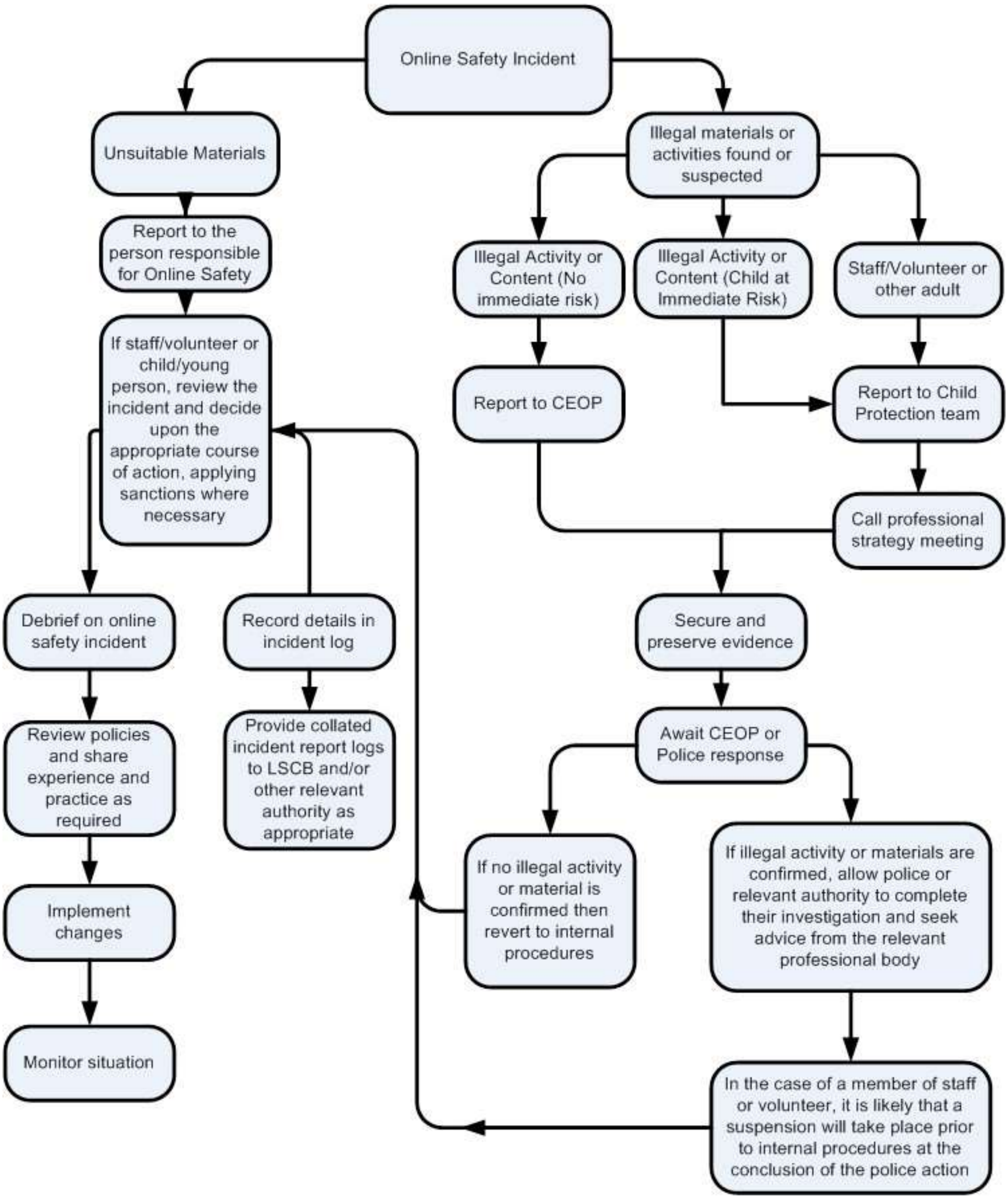
| **User Actions**<br>**Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | ✔ |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | ✔ |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | ✔ |
| 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 | | | | | ✔ |
| Pornography | | | | ✔ | |
| Promotion of any kind of discrimination | | | | ✔ | |
| 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 | | | | ✔ | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy | | | | ✔ | |
| Infringing copyright | | | | ✔ | |
| 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 | | | | ✔ | |
| Unfair usage (downloading / uploading large files that 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 media | | | ✔ | | |
| Use of messaging apps | | | ✔ | | |
| Use of video broadcasting eg Youtube | ✔ | | | | |

## RESPONDING TO INCIDENTS OR MISUSE

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### Illegal Incidents

If there is any suspicion that the website(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 for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

**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.**

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 AND SANCTIONS

It is more likely that each school in 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

| Pupil Incidents | Refer to Class Teacher | Refer to E-Safety Co-ordinator | Refer to Headteacher or Deputy Head | Refer to Police | Refer to ICTDS for action re filtering/ security etc | Inform parents/ carers | Removal of network/ internet access rights | Warning | Further sanction e.g. 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 mobile device | | ✔ | ✔ | | | ✔ | | ✔ | |
| Unauthorised use of social media / messaging apps / personal email | | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | |
| Unauthorised downloading or uploading of files | | ✔ | ✔ | | ✔ | ✔ | ✔ | ✔ | |
| Allowing others to access school network by sharing username and passwords | ✔ | ✔ | | | | | ✔ | ✔ | |
| Attempting to access or accessing the school network, using another pupil's account | | ✔ | ✔ | | | ✔ | ✔ | ✔ | |
| Attempting to access or accessing the school network, using the account of a member of staff | | ✔ | ✔ | | ✔ | ✔ | ✔ | | ✔ |
| Corrupting or destroying the data of other users | | ✔ | ✔ | | ✔ | ✔ | ✔ | | ✔ |
| Sending an email, text or 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 | | ✔ | ✔ | ✔ | | ✔ | ✔ | | |

## Actions / Sanctions

| **Staff Incidents** | Refer to Headteacher or Deputy Head | Refer to Local Authority/ Governors/ HR | Refer to Police | Refer to ICTDS for action re filtering/ security etc | Warning | Possible Disciplinary Action | Possible suspension/ dismissal |
|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | ✔ | ✔ | ✔ | | | ✔ | ✔ |
| Inappropriate personal use of the internet / social media / 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 message that is regarded as offensive, harassment or of a bullying nature | ✔ | ✔ | | | | ✔ | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | ✔ | ✔ | | ✔ | | ✔ | ✔ |
| Actions which could compromise the staff member's professional standing | ✔ | ✔ | | | ✔ | ✔ | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | ✔ | ✔ | | | ✔ | ✔ | |
| Using proxy sites or other means to subvert the school's / academy'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 | ✔ | ✔ | | | | ✔ | |

## 6. ACKNOWLEDGEMENTS

This policy is based on the Template policies by SWGFL, who 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

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2013.  However, SWGfL can not guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.