

The Federation of

Stoke Hill Schools

**E Safety Policy**

**Date agreed: …………………………………**

**Term to be reviewed: ……………………….**

**CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| 1. | Background | ………………………………….. | P2 |
| 2. | Development/Review | ………………………………….. | P3 |
| 3. | Scope of the Policy | ………………………………….. | P4 |
| 4. | Roles and Responsibilities | ………………………………….. | P4 |
| 5. | Policy Statements | ………………………………….. | P7 |
| 6. | Curriculum | ………………………………….. | P9 |
| 7. | Use of Digital Images | ………………………………….. | P9 |
| 8 | Data Protection | ................................................ | P10 |
| 9. | Communications | ………………………………….. | P12 |
| 10. | Unsuitable/Inappropriate activities | ………………………………….. | P14 |
| 11 | Responding to incidents of misuse | ................................................. | P16 |
| 12 | Acknowledgements | ................................................. | P20 |
| 13 | Acceptable User Agreements | ................................................. |  |
|  | Staff, Governors, Visitors | ................................................. | P21 |
|  | Pupils | ................................................. | P22 |
|  |  |  |  |

**Federation of Stoke Hill Schools**

**E-Safety Policy**

**1 Background / Rationale**

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

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupilslearn 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. This e-safety policy helps to ensure safe and appropriate use. The development and implementation of such a strategy involves all the stakeholders in a child’s education from the head teacher 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 achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content

• Unauthorised access to / loss of / sharing of personal information

• The risk of being subject to grooming by those with whom they make contact on the internet.

• The sharing / distribution of personal images without an individual’s consent or knowledge

• Inappropriate communication / contact with others, including strangers

• Cyber-bullying

• Access to unsuitable video / internet games

• An inability to evaluate the quality, accuracy and relevance of information on the internet

• Plagiarism and copyright infringement

• Illegal downloading of music or video files

• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

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.

3

4

**2 Development / Monitoring / Review of this Policy**

This e-safety policy has been developed by a working group / committee made up of:

*• Child protection officers - Sarah Mackay Head teacher (SHINS); Roy Souter Headteacher (SHJS)*

*• Senior Leaders*

*• Teachers*

*• Support Staff*

*• ICT Technical staff*

*• Governors*

Consultation with the whole school community has taken place through the following:

*• Staff meetings*

*• Governors meeting / sub committee meeting*

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This e-safety policy was approved by the *Governing Body / Governors Teaching and Learning Committee on:* | *19th November 2015* |
| The implementation of this e-safety policy will be monitored by the: |  *Senior Leadership Team, ICT Team* |
| Monitoring will take place at regular intervals: | *Once a year -*  |
| The *Governing Body / Governors Teaching and Learning Committee* will receive updates through the head teachers report. | *Every Full 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: | *One year from above date* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Sarah Mackay – Child protection officer and Head teacher (SHINS).**Roy Souter – Headteacher (SHJS)**LADO for LA**LA ICT Manager, LA Safeguarding Officer, Police Commissioner’s Office* |

The school will monitor the impact of the policy using:

*• Logs of reported incidents*

*• SWGfL monitor internet activity (including sites visited)*

*• Technician to run termly health check and inform ICT team of any concerns / issues.*

**3 Scope of the Policy**

6

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

**4 Roles and Responsibilities**

7

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

**4.1 Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors / Governors Curriculum Committee* receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor* (it is suggested that schools consider this being a separate appointment to the ICT Link Governor). The role of the E-Safety Governor will include:

*• regular meetings with the Child protection officer – Head teacher*

*• regular monitoring of e-safety incident logs*

*• regular monitoring of filtering / change control logs*

*• reporting to relevant Governors committee / meeting*

**4.2 Head teacher and Senior Leaders:**

• **The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community**.

*•* The Head teacher / Senior Leaders are responsible for ensuring that staff receive suitable CPD 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 reports from the ICT team and technician.

• **The Headteacher and Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see SWGfL flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / disciplinary procedures)

*•* Termly advice to parents/carers/grandparents/relatives around E-safety and recommended usage of ICT at home.

4.3 Network Manager / Technical staff:

8

*Scomis* is responsible for ensuring:

**• that the school’s ICT infrastructure is secure and is not open to misuse or malicious attack**

**• that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**

**• that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are regularly changed**

• SWGfL is informed of issues relating to the filtering applied by the Grid

*•* the school’s 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 “Filtering Policy Template” for good practice document)

• that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

• that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher / Senior Leader ICT Co-ordinator

9

*•* that monitoring software / systems are implemented and updated as agreed in school policies

**4.4 Teaching and Support Staff**

are responsible for ensuring that:

**• they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**

**• they have read, understood and signed the school Staff Acceptable Use protocol.**

**• they report any suspected misuse or problem to the Headteacher / Leadership Team for investigation**

**• digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) 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 school activities

• pupils understand and follow the school e-safety and acceptable use policy

• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• they monitor ICT activity in lessons, extra curricular and extended school activities

• they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

*•* 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

**4.5 Child Protection Officer**

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

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

Note: 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. Therefore at Stoke Hill we have decided to combine the role of Child Protection Officer and E-Safety Officer.

**4.6 Teaching and Learning Committee ( ICT SIP Team)**

10

Members of *the Teaching and Learning Committee; ICT SIP Team/LT* will assist the *Head teacher with:*

• the review / monitoring of the school e-safety policy / documents.

**4.7 Pupils in KS2:**

**• are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which the Parents/Carers are expected to sign on behalf of the pupil before being given access to school systems.**

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

• will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school

**4.8 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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

**• endorsing (by signature) the acceptable use of internet / ICT for their children in the Infant and Nursery school.**

**At KS2 the Parent/Carer is responsible for ensuring their child understands and signs the Pupil Acceptable Use Policy**

**4.9 Community Users**

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

**5 Policy Statements**

11

**5.1 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 education will be provided in the following ways:

**• A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school**

**• Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**

**• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information**

**• Pupils should be helped to understand the need for the pupil safety and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school**

**• Rules for use of ICT systems / internet will be posted in all classrooms and the ICT suite.**

**• Staff should act as good role models in their use of ICT, the internet and mobile devices**

**5.2 Education – parents / carers**

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

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

• Letters, newsletters, web site.

• Parents evenings

• Reference to the SWGfL Safe website (nb the SWGfL “Golden Rules” for parents)This will be sent out attached to the newsletter on Internet Safety Week(March)

**5.3 Education - Extended Schools**

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

12

**5.4 Education & Training – Staff**

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

• **A programme of formal e-safety training and an audit of e-safety training will also be carried out annually.**

**• All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies**

**• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.**

*•* **The head teacher/LT will provide advice / guidance / training to individuals as required**

**5.5 Training – Governors**

**Teaching and Learning Committee Governors should take part in annual e-safety training / awareness sessions**. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.

• Participation in school training / information sessions for staff or parents

**5.6 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 ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance**

**• There will be regular reviews and audits of the safety and security of school ICT systems**

**• Servers, wireless systems and cabling must be securely located and physical access restricted**

13

• **All users will have clearly defined access rights to school ICT systems.**

• **All users will be provided with a username and password. Pupils will log onto their year group profile. Pupils cannot be identified individually and they will always be closely supervised by a member of staff. For purposes of teaching and learning preparation staff will log onto their own profile and used their own personal password.**

**• The “master / administrator” passwords for the school ICT system are held in the school safe and a copy is held by administrative staff.**

*•* **The school maintains and supports the managed filtering service provided by SWGfL** *–*

*•* **In the event of the need to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher. Office staff (TW and LL) hold the password and access for managing the system.**

**• Any filtering issues should be reported immediately to SWGfL.**

*•* **Requests from staff for sites to be removed from the filtered list will be considered by the Sarah Mackay – Head teacher.**

**If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Teaching and Learning committee**

*• Remote management tools are used by Scomis and St James to manage problems and carry out updates.*

*•* Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

*• An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, visitors) onto the school system by logging on as a pupil according to the year group they are working within. In the case of long term placements e.g. SCITT students then a log on will be provided by the ICT SIP Team, in accordance with the staff protocol.*

14

*• An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school. (See staff protocol)*

*•* The school infrastructure and individual workstations are protected by up to date virus software.

• Teaching staff are provided with an encrypted memory stick for storing pupil / personal data. All laptops are password protected.

 Staff are aware of the need to back up data and clear cameras etc. of pictures of children.

**6 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, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

• At KS2 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

**7 Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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:

**• In KS2 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.**

15

•Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

* Any photos taken to identify H&S risks/maintenance needs need to be free of images of children

•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.

• *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 names will not be used anywhere on a website without prior parental/carer consent.*

• *Written permission from parents or carers will be obtained before photographs of pupils / pupil’s work are published on the school website as part of the consent form for pupil images and internet use signed by parents or carers.*

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

**•** the data must be encrypted and password protected

**•** the device must be password protected

**•** the device must offer approved virus and malware checking software

16

**•** 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

**9 Communications**

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

|  |  |  |
| --- | --- | --- |
|  | Staff & other adults | Students / Pupils |
| Communication Technologies | Allowed | Allowed at lunch 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  |  |  |  | ✓ |  |  |  | ✓ |
| Use of hand held devices eg PDAs, PSPs | ✓, but not in a teaching session. |  |  |  |  | ✓ |
| Use of personal email addresses in school, or on school network |  | ✓ |  |  |  |  |  | ✓ |
| Use of school email for personal emails | ✓ |  |  |  |  |  |  | ✓ |
| Use of chat rooms / facilities |  | ✓ |  | ✓ |  |  |  | ✓ |
| Use of instant messaging |  | ✓ |  |  |  |  |  | ✓ |
| Use of social networking sites |  | ✓ |  |  |  |  |  | ✓ |
| Use of blogs |  | ✓ |  |  |  |  |  | ✓ |

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

**• The official school email service may be regarded as safe and secure and is monitored.**

**• Users need to be aware that email communications may be monitored**

**• Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.**

**• Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

*• at KS2 and above will be provided with individual school email addresses for educational use.*

*•* Pupil should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**10 Unsuitable / inappropriate activities**

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

18

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:**  | **child sexual abuse images** |  |  |  |  | ✓ |
| **promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation** |  |  |  |  | ✓ |
| **adult material that potentially breaches the Obscene Publications Act in the UK** |  |  |  |  | ✓ |
| **criminally racist material in UK** |  |  |  |  | ✓ |
| **pornography** |  |  |  | ✓ |  |
| **promotion of any kind of discrimination** |  |  |  | ✓ |  |
| **promotion of racial or religious hatred**  |  |  |  | ✓ |  |
| **threatening behaviour, including promotion of physical violence or mental harm**  |  |  |  | ✓ |  |
| **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** |  |  |  | ✓ |  |
| **Using school systems to run a private business** |  |  |  | ✓ |  |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school** |  |  |  | ✓ |  |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** |  |  |  | ✓ |  |
| **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)** |  |  |  | ✓ |  |
| **Creating or propagating computer viruses or other harmful files** |  |  |  | ✓ |  |
| **Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet** |  |  |  | ✓ |  |
| **On-line gaming (educational)** |  | ✓ |  |  |  |
| **On-line gaming (non educational)** |  |  |  | ✓ |  |
| **On-line gambling** |  |  |  | ✓ |  |
| **On-line shopping for school resources**  |  | ✓ |  |  |  |
| **File sharing** | ✓ |  |  |  |  |
| **Use of social networking sites** |  |  |  | ✓ |  |
| **Use of video broadcasting in accordance with the school filtering system**19 | ✓ |  |  |  |  |

**11 Responding to incidents of misuse**

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

**If any apparent or actual misuse appears to involve illegal activity ie.**

**• child sexual abuse images**

**• adult material which potentially breaches the Obscene Publications Act**

**• criminally racist material**

**• other criminal conduct, activity or materials**

**the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.aspshould be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.**



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL “Procedure for Reviewing Internet Sites for Suspected Harassment and Distress” should be followed. This can be found on the SWGfL Safe website within the “Safety and Security booklet”. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

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

20

|  |  |
| --- | --- |
| Pupils | Actions / Sanctions  |
| Incidents: | Refer to class teacher / tutor | Refer to Head of Department / Head of Year / other | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering / security etc | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion  |
| **Deliberately accessing or trying to access material that could be considered illegal**  | ✓ | N/A | ✓ | ✓ | ✓ |  |  |  | ✓ |
| Unauthorised use of non-educational sites during lessons | ✓ | N/A | ✓ |  | ✓ |  |  |  | ✓ |
| Unauthorised use of mobile phone / digital camera / other handheld device | ✓ | N/A | ✓ |  |  | ✓ |  |  | ✓ |
| Unauthorised use of social networking / instant messaging / personal email | N/A |
| Unauthorised downloading or uploading of files | ✓ | N/A | ✓ |  | ✓ | ✓ |  |  | ✓ |
| Allowing others to access school network by sharing username and passwords | N/A |
| Attempting to access or accessing the school network, using another student’s / pupil’s account | N/A |
| Attempting to access or accessing the school network, using the account of a member of staff | N/A |
| Corrupting or destroying the data of other users | ✓ | N/A | ✓ |  | ✓ | ✓ |  |  | ✓ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | N/A |
| Continued infringements of the above, following previous warnings or sanctions | N/A |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | N/A |
| Using proxy sites or other means to subvert the school’s filtering system | N/A |
| Accidentally accessing offensive or pornographic material and failing to report the incident | ✓ | N/A | ✓ |  | ✓ | ✓ |  | ✓ |  |
| Deliberately accessing or trying to access offensive or pornographic material | ✓ | N/A | ✓ |  | ✓ | ✓ |  |  | ✓ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act21 | N/A |

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

**12 Acknowledgements**

22

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:

• Members of the SWGfL E-Safety Group and the SWGfL E-Safety Conference Planning Group

• Avon and Somerset Police

• Somerset County Council

• Plymouth City Council

• Swindon Borough Council

• Poole Borough Council

• Bournemouth Borough Council

• North Somerset Council

• Gloucestershire County Council

• DCSF

• Becta

• National Education Network (NEN)

• London Grid for Learning

• Kent County Council

• Northern Grid for Learning

• Bracknell Forest Borough Council

• Byron Review – Children and New Technology – “Safer Children in a Digital World”

Date on which policy was approved: 12th January 2012

Reviewed by T & L Nov 15

This policy will be reviewed annually on (date): November 2016

Copyright of the SWGfL School E-Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2009. However, SWGfL can not guarantee it’s accuracy, nor can it accept liability in respect of the use of the material.

**Federation of Stoke Hill Schools**

**Staff, Governor and Visitor**

**Acceptable Use Agreement / Code of Conduct**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school ICT coordinators or the Head teacher.

* I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Head or Governing Body.
* I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
* I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
* I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
* I will only use the approved, secure e-mail system(s) for any school business.
* I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
* I will not install any hardware of software without permission of the Head teacher or ICT Coordinator
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
* I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
* I will respect copyright and intellectual property rights.
* I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
* I will support and promote the school’s e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
* I understand this forms part of the terms and conditions set out in my contract of employment.

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….………………….………… Date ……………………

Full Name ………………………………….........................................(printed)

**Federation of Stoke Hill Schools**

**Primary Pupil Acceptable Use**

**Agreement / eSafety Rules**

* I will only use ICT in school for school purposes.
* I will only use my class e-mail address or my own school e-mail address when e-mailing.
* I will only open e-mail attachments from people I know, or who my teacher has approved.
* I will not tell other people my ICT passwords.
* I will only open/delete my own files.
* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
* I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
* I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
* I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
* I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
* I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

****

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the Headteacher

**✂**

**Parent/ carer signature**

We have discussed this and ……………………………………..........(child name) agrees to follow the eSafety rules and to support the safe use of ICT at the Federation of Stoke Hill Schools.

Parent/ Carer Signature …….………………….………………………….

Class …………………………………. Date ………………………………