SOUTH WEST SWSFS’ FEDERATION
E –SAFETY POLICY

Rationale

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

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 SWSFs are bound. This e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in SWSF 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 SWSF. 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 SWSF 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 SWSF 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.

Scope of the Policy

SOUTH WEST SWSFS' FEDERATION
E –SAFETY POLICY

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

The Education and Inspections Act 2006 empowers Head of SWSFs, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the SWSF 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 SWSF, but is linked to membership of the SWSF.

The SWSF 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 SWSF.

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.

Heads of SWSF and Senior Leaders:

- The Head of SWSF is responsible for ensuring the safety (including e-safety) of members of the SWSF community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator / Officer.
- The Head of SWSF / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Head of SWSF / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in SWSF 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 Head of SWSF and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see SWGfL flow chart on dealing with e-safety incidents – "Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the SWSF 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 SWSF ICT technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

Network Manager / Technical staff:

The ICT Technician / ICT Co-ordinator is responsible for ensuring:

- that the SWSF's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the SWSF 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 SWSF'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
- 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

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current SWSF e-safety policy and practices
- they have read, understood and signed the SWSF Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator / Officer /Head of SWSF / Senior Leader / Head of ICT / ICT Co-ordinator / Class teacher / Head of Year (as in the section above) for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level
- e-safety issues are embedded in all aspects of the curriculum and other SWSF activities
- pupils understand and follow the SWSF 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 SWSF 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 SWSF 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

Pupils:

- are responsible for using the SWSF ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to SWSF 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 SWSF policies on the use of digital cameras and hand held devices. They should also know and understand SWSF 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 SWSF and realise that the SWSF's E-Safety Policy covers their actions out of SWSF, if related to their membership of the SWSF

Education – pupils

The education of pupils in e-safety is an essential part of the SWSF's e-safety provision. Children and young people need the help and support of the SWSF 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 SWSF and outside SWSF
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Education – parents / carers

Parents and carers 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 SWSF will therefore seek to provide information and awareness to parents and carers through:

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

Parents and carers will be responsible for:

- supporting the SWSF in their child's education of e-safety.

Technical – infrastructure / equipment, filtering and monitoring

The SWSF will be responsible for ensuring that the SWSF 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:

- SWSF ICT systems will be managed in ways that ensure that the SWSF 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 SWSF ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to SWSF ICT systems.
- All users (at KS2 and above) will be provided with a username and password
- The "master / administrator" passwords for the SWSF ICT system, used by the Network Manager (or other person) must also be available to the Head of SWSF or other nominated senior leader and kept in a secure place (eg SWSF safe)
- The SWSF maintains and supports the managed filtering service provided by SWGfL
- 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 SWSF systems and data.

Communications

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

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

- The official SWSF 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 SWSF policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that SWSF ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The SWSF will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use SWSF 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.

For my own personal safety:

- I understand that the SWSF will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the SWSF ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of SWSF:

- I understand that the SWSF also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of SWSF and where they involve my membership of the SWSF community
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the SWSF network / internet, suspensions, contact with parents..

SOUTH WEST SWSFS' FEDERATION
E –SAFETY POLICY

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Policy (AUP), to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to SWSF ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the SWSF ICT systems and equipment (both in and out of SWSF)
- I use my own equipment out of SWSF in a way that is related to me being a member of this SWSF e.g. communicating with other members of the SWSF, accessing SWSF email, VLE, website etc.

Name of Student / Pupil

Class

Signed

Date

Staff (and Volunteer) Acceptable Use Policy Agreement

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 SWSF 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 SWSF 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 SWSF 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 SWSF 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 SWSF ICT systems (eg laptops, email, VLE etc) out of SWSF.
- I understand that the SWSF 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 SWSF.
- 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 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 SWSF 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 SWSF'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 SWSF website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official SWSF systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

SOUTH WEST SWSFS' FEDERATION
E –SAFETY POLICY

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in SWSF, I will follow the rules set out in this agreement, in the same way as if I was using SWSF equipment. I will also follow any additional rules set by the SWSF 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 open any attachments to emails, unless the source is known and trusted, 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 SWSF 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
- I will not disable or cause any damage to SWSF 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 SWSF / LA Personal Data Policy. Where personal data is transferred outside the secure SWSF network, it must be encrypted.
- 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 SWSF 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.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of SWSF ICT equipment in SWSF, but also applies to my use of SWSF ICT systems and equipment out of SWSF and my use of personal equipment in SWSF or in situations related to my employment by the SWSF.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

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

Staff / Volunteer Name

Signed

Date