ST. FLORENCE VC SCHOOL

Believe, Achieve and Succeed Together

E-Safety Policy

St. Florence VC School

E-Safety Policy

Developing / Monitoring and Reviewing of this Policy

The school's e-safety policy has been written by the school, building on the Pembrokeshire e-safety policy guidelines and government guidance. It has been agreed by the senior management and approved by school governors.
This e-safety policy has been developed by a working group made up of Mrs Julie Davies (Head-teacher), Mr James Allen (ICT Co-ordinator), Mrs Jocelyn Morris (Chair of Governors).

Schedule for Development / Monitoring and Review

This e-safety policy was approved by the staff and governing body:	Date
The implementation of this e-safety policy will be monitored by the:	Mr James Allen (ICT Co-ordinator) Mrs Julie Davies (Head-teacher) Mrs Jocelyn Morris (Chair of Governors)
Monitoring will take place at regular intervals:	On a yearly basis
The *Governing Body* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	On a yearly basis, every Summer Term
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:	Spring Term
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LEA ICT Manager, LEA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents

Scope of the policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

E-Safety / ICT Co-ordinator:

- Lead the e-safety committee

- Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents at Governors' meetings, every Summer Term.
- Ensure 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 - Pembrokeshire County Council (PCC)
- Liaises with school staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with Mrs Julie Davies and Mrs Jocelyn Morris to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant Governor's meetings
- Any incidents will be dealt with by the Head-teacher and Chair of Governors with LEA support if needed.

Network Manager and Technical Staff

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy e.g. PGFL. Hwb, encrypted sticks, school computers
- The filtering policy, is applied and updated on a regular basis by the LA

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- All digital communications with students / pupils / 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 developing understanding of research skills
- 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 / Safeguarding Designated Officer

The designated person for child protection 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

(NB: 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. Some schools may choose to combine the role of Child Protection Officer / Safeguarding Designated Person and E-Safety Officer)

Contact Numbers
Child Care Assessment Team
(CCAT)
Duty Social Worker Desk
01437 77 6322 or **6325** or **6444**
Out of Hours **08708 509508**

Local Authority Designated
Officer for Allegations (LADO)
01437 77 6696/6562

E-Safety Group

Mrs Julie Davies (Head-teacher)
Mr James Allen (ICT Co-ordinator)
Mrs Jocelyn Morris (Chair of Governors)
2 year 6 digital leaders

The E-Safety Group provides a consultative group that has a representation from the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Members of the E-safety Group will assist the ICT Coordinator and Headteacher, with:

- The production / review / monitoring of the school e-safety policy / documents.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- Monitoring improvement actions identified through use of the 360 degree safe self review tool.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy.
- Have a developing understanding of research skills.
- 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 / 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/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, school website, HWB and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.
E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum – Digital Literacy and Citizenship SWGL **(www.swgfl.org.uk/digitalliteracy)** should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of classroom activities and assemblies e.g. during e-safety week
- 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 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 young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the LEA 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 auditable, with clear reasons for the need.

Parents / Carers

Many parents and carers may only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings
- High profile events / campaigns e.g. Internet Safety Week
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Staff and Volunteers

It is essential that all staff understand their responsibilities, as outlined in this policy.

- All new staff should ensure that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The ICT Co-ordinators will receive regular updates through attendance at external training events (e.g. from SWGfL / LEA / HWB) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The ICT Co-ordinators will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the LEA/National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – Infrastructure / equipment, filtering and monitoring

The School's Service level agreement is provided by the LEA Pembrokeshire County Council.
Refer to PCC Service Specification for ICT Service (Primary).
Internet filtering in Pembrokeshire
Filtering in Pembrokeshire is currently based on the RM Safetynet system and, from September 2014, this will be updated to Smoothwall which will provide more effective and flexible web filtering. Each school currently has its own RM Safetynet system. Filtering management is handled by Pembrokeshire County Council in the case of primary schools, and by school-based staff in secondary schools. All schools receive a nightly update of banned sites from Pembrokeshire County Council, which can be easily supplemented by the relevant technical staff.

- Walled garden (LA filter system). Users are only allowed to visit sites expressly 'allowed' by the LA.
- Filtered. RM Safetynet uses a range of techniques to reduce the possibility of users visiting inappropriate sites.
- Unfiltered. The system does not apply any filtering. RM Safetynet and Smoothwall offer a range of tools to control access to the Internet and to inform/support the school's disciplinary policy. Advice and assistance is available from Pembrokeshire IT consultants.
- The school will work with Pembrokeshire County Council, taking into account Welsh Government guidelines, to ensure that systems to protect pupils are regularly reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-safety officer and forwarded to Pembrokeshire IT Services helpdesk immediately for distribution to all school systems.
- All internet access in the school is filtered. In rare circumstances, there is a valid need to overcome technical limitations through the use of an unfiltered connection. The head teacher should personally authorise all unfiltered Internet users, and review the need for access regularly.
- The school uses a mixture of Walled Garden and Filtered access, appropriate to age, to support pedagogical objectives.
- The school's e-safety policy ties in closely with the LA disciplinary policy.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies.
- The school's filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by technicians and Pembrokeshire IT Consultants.
- Relevant staff will provide users of HWB, mathletics and spellodrome with a username and secure password by ICT Co-ordinators who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.

- Relevant staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. See PCC statements above.

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 students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office (http://www.ico.gov.uk/), 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 / 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 students / 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 students / pupils are published on the school website this covered as part of the AUA signed by parents on entry to the school.
- 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.

The School has adopted the LEA Data Protection policy. (A copy can be found at school)

The Pembrokeshire Data Protection policy will be available on www.pembrokeshire.gov.uk. Another excellent source of information is available from the Information Commissioner's Office: http://www.ico.gov.uk/
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.

Communications

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

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students/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 e.g. HWB. Personal email addresses, text messaging or social media must not be used for these communications.
- 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

- The school will block / filter access to social networking sites. (The Pembrokeshire filtering service currently blocks access to many social networking sites. However schools have a responsibility to report any additional sites that they need filtered / blocked).
- Inappropriate forums (such as Newsgroups) will be blocked.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends, specific interests and clubs etc.
- The school has an acceptable use policy for staff which ensures that staff is aware of the guidelines for the use of mobile phones, email and social networking.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when space has been setup without a password and others are invited to see the bully's comments.

Unsuitable / Inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school / academy 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.

Responding to incidents of misuse

Misuse of electronic equipment
Misuse can be a serious disciplinary offence. Employees MUST NOT use school equipment (including a school provided laptop or mobile devices) to:

Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred

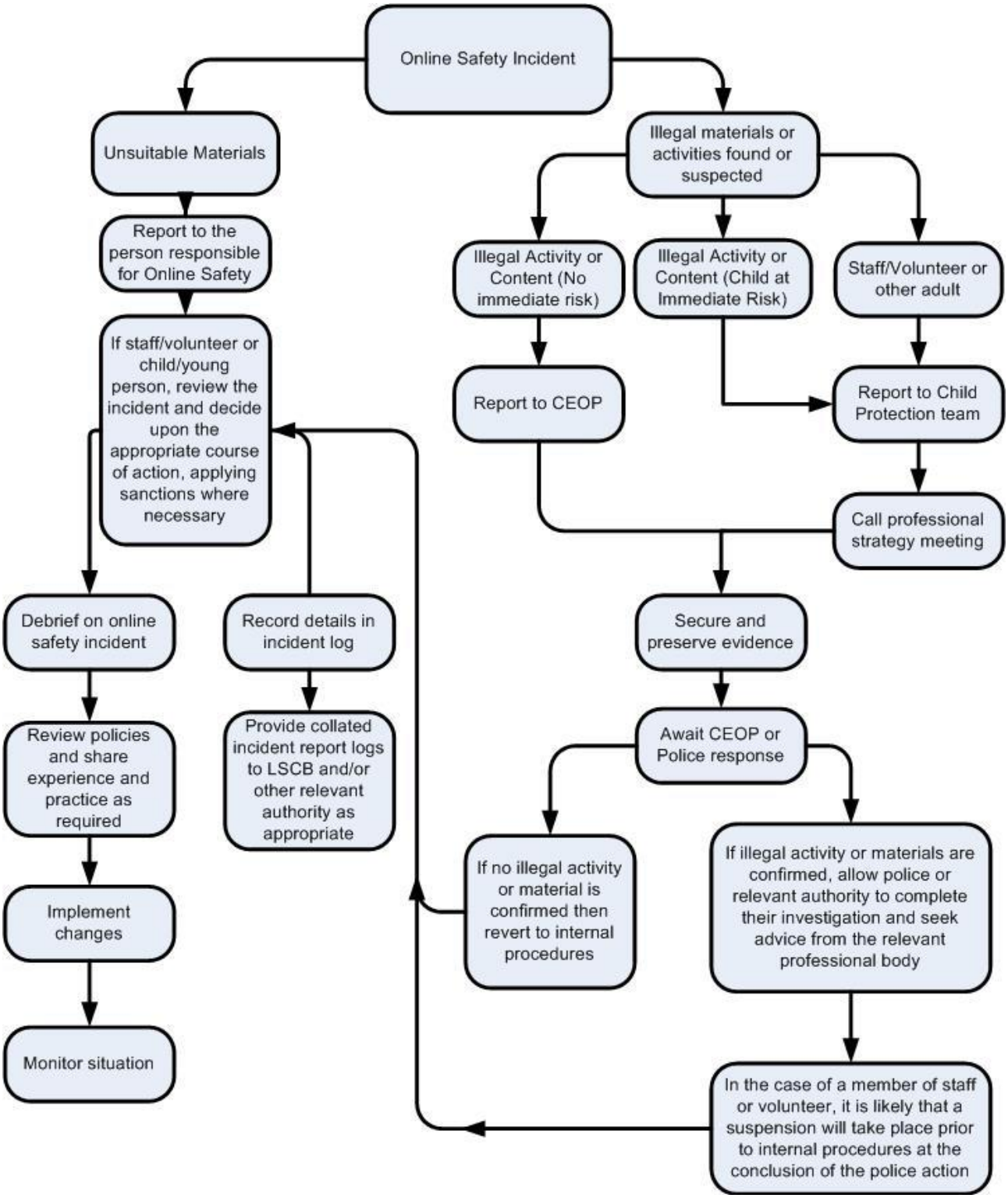
- Gamble
- Undertake political lobbying
- Promote or run a commercial business
- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright
- Spend school time on personal matters (for example, arranging a holiday, shopping, looking at personal interest websites). This may be treated as fraud.
- Store personal information on the school network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper)
- Send emails, texts or messages or publish anything on a website, social networking site or blog, which:
- Is critical about members of the school community including pupils
- Contain specific or implied comments you would not say in person
- *C*ontain inappropriate comments which could cause offence or harassment on the grounds of
- *G*ender, race, disability, age, religion or sexual orientation
- Have originated from a chain letter
- Conduct private and intimate relationships via school systems
- Download or copy software (excluding software updates) or use the email system to transmit any documents or software without checking copyright or licence agreement
- Install software licensed to the school on a personal computer unless permission to do so is explicitly covered by the school licence agreement.
- Take, transmit or publish pictures of a member of staff or pupil on a mobile phone, camcorder or camera without the person's permission
- Give away email lists for non-school business. If in doubt, ask your manager/Head teacher.
- Use internet chat rooms (other than the secure, moderated facilities which are provided within the school's Learning Platform)

Additionally employees MUST NOT:

- Do anything which brings the school or Council into disrepute
- A personal laptop or mobile device brought onto the school premises MUST NOT be used to undertake any of the above activities during the school day, nor should it have information stored within it which would be deemed to be unacceptable on a school machine. It is recommended that a personal laptop used at school should have a separate secure account for school use. Additionally a personal laptop used for any school activity must be fully protected against virus infection.

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff 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.

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

All staff should sign an Acceptable Use Agreement on appointment. Staff, thereby, accept that the school can monitor network and Internet use to help ensure staff and pupil safety. Procedures must define how inappropriate or illegal ICT use is reported to senior management. Staff must be aware of dangers to themselves in managing ICT use, for instance in viewing inappropriate images to investigate their source, and ensure that appropriate safeguards are in place to protect themselves.
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. In industry and indeed in Pembrokeshire County Council, a member of staff who flouts security advice, or uses e-mail or the Internet for inappropriate reasons risks disciplinary procedures. 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. Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action against staff in accordance with the school’s and Council’s disciplinary policy, which may result in dismissal.

Name: **Mrs Julie Davies**

Signature: JA Davies

Date:

Agreed by Governors

Name:

Signature:

Date:

School Council:

Signature: Date:

Signature: Date:

Signature: Date:

Signature: Date:

Signature: Date:

Signature: Date:

Signature: Date:

Staff: Please date