Pembrokeshire County Council

Pembrokeshire County Council e-Safety Strategy and Policy Guidance for Schools

2013 - 2016

www.pembrokeshire.gov.uk

Pembrokeshire County Council believes that the use of information and communication technologies in schools brings great benefits. Recognising the e-safety challenges and planning accordingly will help to ensure appropriate, effective, safe and positive use of electronic communications.

This strategy and policy template will help schools to discuss the issues involved and review their e-safety policy.

The aim of this document is to assist Pembrokeshire schools in formulating an effective and robust e-learning policy.

Executive Summary

The use of information and communication technologies (ICT) including the Internet and related technologies has developed greatly in recent years and now involves every pupil and member of staff. Whilst such powerful technologies have great benefits and advantages they also present users with a number of challenges and there is a need to consider carefully the issues raised by the use of these powerful technologies.

There is a need therefore to ensure that all schools have a current and considered e-safety policy. It is important that all staff are fully aware of online risks and that schools ensure that they meet the e-safety challenges in a positive and practical way. It is essential that schools can turn e-safety policy into effective practice.

Pupils are conversant and practiced in the use of social networking websites, instant messaging programs, text and mobile use. However, many young people lack an appreciation of some of the online challenges and do not fully appreciate the consequences of their on line actions and behaviour. It is vital therefore that both pupils and staff are protected by robust e-safety policies and practice.

There are a number of Government initiatives that seek to raise awareness and protect pupils from on-line dangers including those of Welsh Government (HWB) and the Child Exploitation and Online Protection centre (CEOP). Other organisations such as Child Net, UK Safer Internet Centre and Wisekids are also very active in this area.

It is important therefore that all schools make e-safety a priority. This guidance has been produced as a result of collaboration between Carmarthenshire and Pembrokeshire's School Improvement Service and IT Services with the assistance of a panel of head teachers from Pembrokeshire schools, Education and Children's Services, Pembrokeshire's Data Protection and Legal Departments and Dyfed Powys Police.

CONTENTS

1.0 e-Safety Self Review

The self review is designed to help you evaluate current practice in e-safety.

In each section we have outlined 3 levels for schools to measure their current practice against - Developing, Establishing and Enhancing. Alongside these, we have listed key actions a school could take to move through the levels, as well as the support available from Pembrokeshire County Council to help deliver improvements.

The levels are designed to be challenging. Level 3 (Developing) sets the basic expectations schools should have regarding that area of e-safety. Level 2 (Establishing) is the National ICT Mark standard. Level 1 (Enhancing) demonstrates best practice, building further on the ICT Mark standard.

The self review elements are taken from Naace ICT self review framework for schools. The ICT advisory team recommend that all schools use the ICT self review framework to enable effective delivery of ICT for teaching, learning and e-safety and review progress with reference to national standards. Full details of the self review can be found online at: www.naace.co.uk/ictmark/srf

Schools interested in going further and undertaking a comprehensive self-review of e-safety can use the South West Grid For Learning 360 Degree Safe self-review tool at: www.swgfl.org.uk/Staying-Safe/360-degree-safe

Element a - Policies and practice

Level 3 (Developing)

The school is fully aware of its responsibilities and takes appropriate action to ensure that ICT usage by all staff and pupils is responsible, safe and secure.

It has a co- ordinated approach to the development and implementation of its e- safety policy.

Level 2 (Establishing)

E-safety is embedded within the wider school culture.

Policies are comprehensive and regularly reviewed in line with developments in technology and practice.

There is co-ordinated and robust implementation of e-safety policies by all staff, governors and pupils within and beyond the school and practice is monitored.

The school engages regularly with parents/carers to promote the e-safety of pupils beyond the school.

Level 1 (Enhancing)

The school is vigilant in identifying and responding to new challenges for e-safety.

Through constructive dialogue it encourages pupils, parents/carers, other stakeholders and the wider community to contribute to ongoing developments in e-safety policy and practice, and helps them to deal with e-safety challenges they encounter.

The following actions would help a school progress towards Level 1 (Enhancing):

1. Ensure that a fully consulted e-safety and acceptable use policy is in place, and that it is updated annually.
2. Ensure that all staff handbooks have an e-safety incident management flow chart and that e-safety incidents are recorded.
3. Ensure that all staff and volunteers understand how to respond to an e-safety concern.
4. Have a designated e-safety Officer.
5. Monitor the effectiveness of the policies into practice.

To support schools, the LA will:

1. Offer advice and guidance on policy development.
2. Offer advice on policies prior to adoption.
3. Offer e-safety support to schools using the South West Grid for Learning 360° Safe Framework and/or the Naace ICT Self Review Framework.
4. Offer CEOP Thinkuknowtraining to schools as a child protection Tier 3 module.
5. Provide a growing resource of self-help materials for three specific audiences - children and young people, parents and professionals.
6. Engage with the Junior Local Safeguarding Board (Junior Safeguardians) and ensure they have an active voice in the Pembrokeshire e-Safety Group.
7. Explore and engage with new technologies to promote the e-safety message as widely as possible.
8. Provide support to schools for the annual Safer Internet Day and run an annual competition to raise awareness of the event.

Element b - Planning for e-safety

Level 3 (Developing)	**Level 2 (Establishing)**	**Level 1 (Enhancing)**
Planning provides opportunities for pupils to develop an awareness of some aspects of e-safety and some of the skills needed to make safe and responsible use of ICT.	Effective planning ensures that pupils have the opportunities to develop both an awareness of e-safety issues and the skills that enable them to make safe and responsible use of ICT.	Systematic planning ensures that all pupils have opportunities to develop both an understanding of e- safety issues and a range of e-safety strategies, skills and behaviours. Plans are regularly reviewed and updated in the light of changing technology and practice.

The following actions would help a school progress towards Level 1:

1. Ensure that e-safety incidents are logged, acted upon and reviewed by the school's e- safety officer.
2. Headteacher reports to the school governing body should include a report on e-safety activity to include updates on training, policy and practice, as well as e-safety incidents.
3. Have a scheduled e-safety update during INSET sessions annually with all staff.

To support schools, the LA will:

1. Offer email/telephone advice and guidance to schools on e-safety incidents.
2. An e-safety summary will be included in the LA Section 175 annual report to the Head of Education.
3. Deliver e-safety training in schools.
4. Provide a flowchart which clearly demonstrates the procedure for managing e-safety incidents in school.
5. Provide timely advice and guidance to schools when trends in e-safety issues are identified.

Element c - Understanding the risks

Level 3 (Developing)	Level 2 (Establishing)	Level 1 (Enhancing)
Most pupils are aware of the issues and risks involved in the use of ICT and are aware of school policy and the need to adopt appropriate and responsible behaviours. However, not all pupils have sufficient knowledge and skills to enable them to make safe and effective use of digital resources.	All, or nearly all, pupils understand the issues and risks involved in the use of ICT. They are aware of school policy and the need to adopt appropriate and responsible behaviours. Most pupils have a good range of knowledge and skills to enable them to make safe and effective use of resources both within and beyond the school. Pupils know where to go for support if they are concerned about any e-safety issue.	All, or nearly all, pupils consistently adopt safe practices both within and beyond the school. They have a full range of knowledge and skills to ensure safe and effective use of a wide range of digital resources. They apply and adapt these to new and emerging technologies.

The following actions would help a school progress towards Level 1:

1. Promote the annual Safer Internet Day available to all stakeholders.
2. Consult with pupils, parents and carers annually on e-safety matters.
3. Provide opportunities for stakeholders to have input into policy development.

To support schools the LA will:

1. Offer support to schools in engaging with stakeholders.
2. Offer a range of e-safety resources to schools.
3. Develop regular communications with schools to highlight current trends and associated risks.

Element d - Monitoring data security

Level 3 (Developing)	Level 2 (Establishing)	Level 1 (Enhancing)
Technical solutions provide some safeguarding for users of the school's ICT systems. These sometimes limit opportunities for learning and teaching. The school is taking steps to ensure that data is secure both on and off site - e.g. by ensuring that laptops and mobile devices are password protected and hard drives are encrypted.	Regularly updated technical solutions ensure a safe environment for all users whilst maximising learning and teaching opportunities. There is a high level of data security on all systems with timely and effective disaster recovery.	Technical solutions ensure that there is safeguarding of the school's ICT systems, without limiting opportunities for learning and teaching. Data is stored securely on and off site and regular reviews ensure that these systems remain effective.

The following actions would help a school progress towards Level 1:

1. Provide information to the IT Helpdesk (hd@pembrokeshire.gov.uk) regarding any data security issues that may occur.
2. Ensure that the school is informed of the latest developments and can show that these have been considered in relation to the school development plan.
3. Audit the reality of data in transit across the school. Schools should understand how staff move data around, by what method and with what safeguards.
4. Participate in ongoing training and awareness raising.
5. Where filtering is managed locally, ensure a senior manager approves the school filtering configuration and supervises the staff who manage it.

To support schools, the LA will:

1. Ensure there is always advice and guidance on data security available.
2. Promote a means of transporting data securely.
3. Provide timely advice and guidance where trends are identified.
4. Ensure that the latest advice and guidance from CEOP is available and signpost schools to a CEOP trained ambassador.

2.0 Responding to an Incident of Concern

Internet technologies and electronic communications provide children and young people with opportunities to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with the way these technologies can be used.

An e-safety policy should recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for others.

These risks to e-safety are caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to considered illegal activity.

This section will help staff determine what action they can take and when to report an incident of concern to the person with responsibility for child protection or e-safety within the school. Following consultation with the head teacher matters can then be referred to the Local Authority Child Protection Designated Officer (LADO) or to the Police if that is deemed necessary.

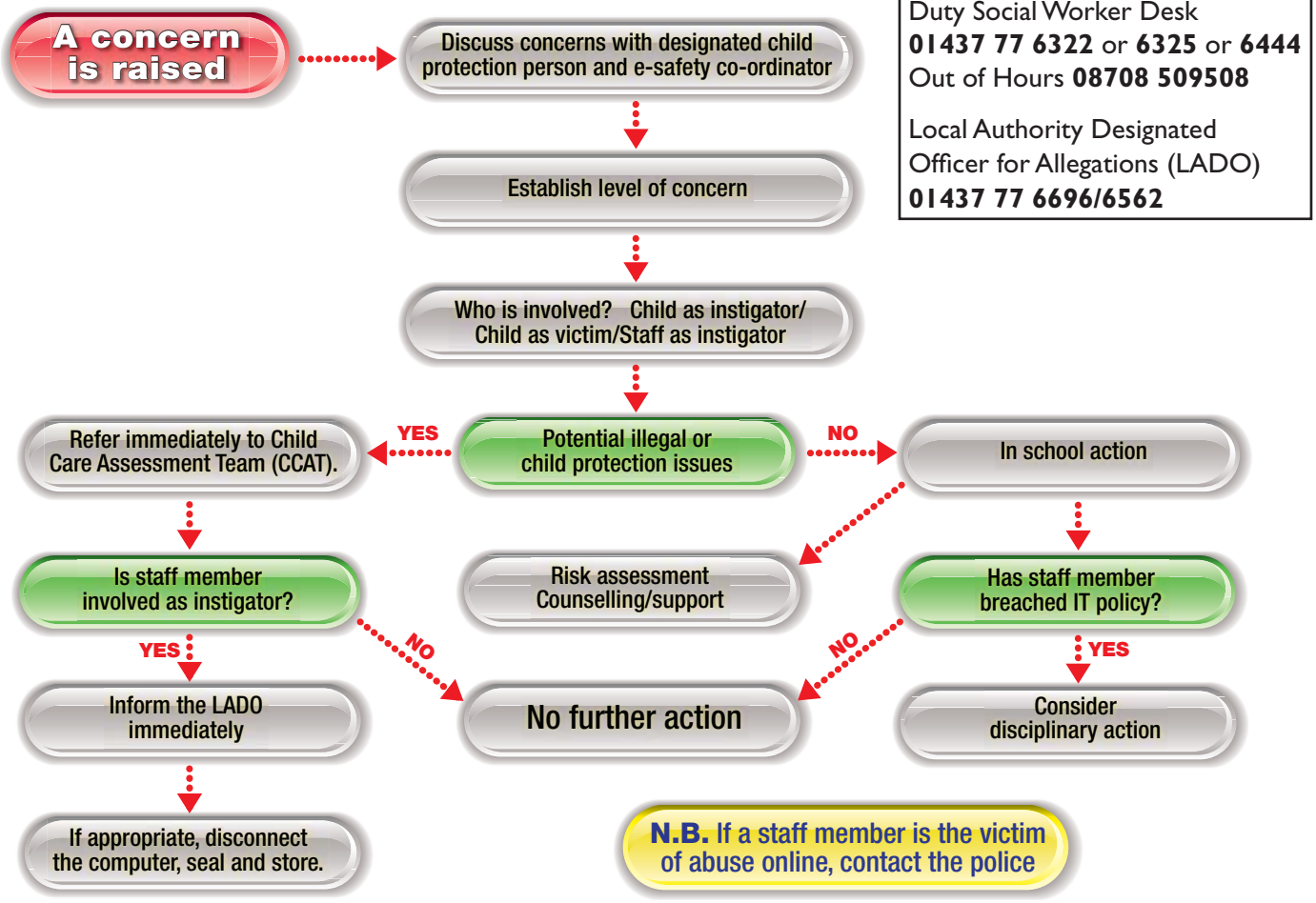
The child protection or e-safety officer can provide guidance should a member of staff be concerned about the Internet use made by a child, young person or member of staff.

The flowchart below illustrates the approach to resolving an incident of concern. This diagram should not be used in isolation but in line with the school's child protection policy and procedures.

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



3.0 Writing a School e-Safety Policy

3.1 Why write an e-safety policy?

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved within the limitations of the available technology are great but can on occasions, place young people in vulnerable situations.

Schools need to decide on the right balance between controlling access, setting rules and educating students for responsible use. Parents, libraries and youth organisations must also develop complementary strategies to ensure safe, critical and responsible ICT use wherever young people may be accessing these technologies.

This guidance has been formulated to provide support to schools regarding the formulation of a robust, practical and positive e-safety policy.

E-safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Detailed e-safety materials and guidance for schools are available from the HWB Learning Platform, the Child Exploitation and Online Protection Centre (CEOP), Dyfed-Powys Police School Liason Service, NSPCC, Childline, Beat Bullying, the South West Grid for Learning and other agencies.

3.2 What is e-safety?

The School's e-safety Policy reflects the need to raise awareness of e-safety issues associated with all information systems and electronic communications as a whole.

E-safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences in a safe and positive way.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information can compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

3.3 How do I use the policy template?

Teachers will be aware of the risks of Internet use but may not have had opportunities for detailed discussion. The policy template provides a structure for policy writing and material to stimulate and widen this essential debate.

When writing your policy, educational, management and technical issues will need to be considered. These are presented as questions with discussion and a range of suggested statements. There is a need to consider each question and select statements appropriate to the school context or modify or replace any statement.

Some schools may feel they do not have the expertise to write their own policy. Pembrokeshire County Council has also published core policies for primary and secondary schools on the Education Portal that can be edited relatively quickly for approval by managers and governors. However in all cases careful consideration of the needs of your individual school must be given when developing your e-safety policy.

As guidance in areas such as e-mail, social networking and publishing continues to evolve schools should also consult the Welsh Government guidance published on the HWB All Wales Learning Platform. Schools should review their policy regularly and revise the policy annually to reflect changes and advancements in technology. School ICT use is changing rapidly and policies produced a year ago may already need revision.

3.4 Statement of authority

This document has been written to reflect effective practice, to raise issues and to point to sources of expert knowledge and support. A number of people have contributed to this guidance, including the Pembrokeshire e-Safety Group, Dyfed-Powys Police, and Carmarthenshire School Improvement Service.

National agencies such as HWB and CEOP have also been consulted and their materials referenced. Through this guidance, the Authority is making a strong statement as to the mechanisms that it expects schools to put in place to protect pupils. Schools basing their e-safety policies on this guidance will be able to demonstrate more easily that they have taken reasonable steps to ensure the protection of pupils.

Schools have the immediate responsibility for e-safety and must consider the issues raised in this document. An e-safety audit is recommended, possibly using external expertise, to help ensure that all reasonable steps have been taken.

This is not, of course, your school's e-safety policy. That should be written by the head teacher in consultation with relevant staff after reviewing this document, consulting the reference material and discussing what is appropriate in your school.

3.5 Responsibilities of school staff

Information technologies are developing rapidly and can leave staff unsure of best practice or how to discuss e-safety issues with pupils. Advice and training may be obtained from School Improvement Service or Pembrokeshire Schools IT Consultants.

The trust between pupils and school staff is essential to education but very occasionally pupils can feel uncomfortable in discussing certain issues with staff. This is not new, but has been highlighted by better awareness of human failings and greater respect for children. Nationally, CEOP has been set up by the Home Office to "safeguard children's online experiences and relentlessly track down and prosecute offenders".

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.

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.

Staff that manage filtering systems or monitor ICT use have great responsibility and must be appropriately supervised. 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.

Any allegation of inappropriate behaviour must be reported to senior management and investigated in line with Section 2 'Responding to an Incident of Concern'.

3.6 School responsibilities

- Pembrokeshire County Council expects schools to appoint a senior member of staff with an e-safety role.
- It is essential that all staff in schools adhere to the Electronic Communication and Social Media policy (see Section 5).
- The headteacher's report to governing body should include a summary of e-safety activity, including updates on policy, practice, training and e-safety incidents.
- The e-safety officer should maintain the e-safety policy, manage e-safety support and keep abreast of local and national e-safety awareness campaigns.
- Schools should review their policy regularly and revise their policy annually to ensure that it is current and considers any emerging technologies.
- Schools should audit their filtering systems regularly to ensure that inappropriate websites are blocked. In Primary schools this will be done in cooperation with the IT Consultant for Primary schools and Pembrokeshire IT Services.
- To ensure that pupils and staff are adhering to the policy, any incidents of possible misuse should be investigated.
- Schools should ensure that e-safety is an integral part of the curriculum and that every pupil has been well-informed regarding safe and responsible use. Pupils need to know how to control and minimise online risks and how to report a problem.
- All staff must read and sign the Acceptable Use Policy for Staff / Corporate Policy for staff.
- The e-safety policy should be made available to all staff, governors, parents and visitors.
- All schools should ensure pupil participation in e-safety by electing pupil e-safety champions, who will promote e-safety and work with the school to develop best practice. Displaying pupil designed posters in classrooms is one useful approach and many schools include e-safety guidelines in Home School Contact Books.

4.0 e-Safety Policy Development

4.0 E-Safety Policy Development

Document format: A question invites discussion followed by recommended guidance statements for schools to use in the preparation of their e-safety policy.

Selection is important as statements cover a wide variety of situations and some may be inappropriate for your school. Naturally schools may edit the statements or substitute their own.

4.1 Who will write and review the policy?

Discussion: *The e-safety policy is part of the ICT policy and School Development Plan and should relate to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Policy construction provides a method to review practice, in this case the use of a major technology and its benefits and risks. The more that staff, parents, governors and pupils are involved in deciding the policy, the more effective it will be.*

Possible statements:

- The school will appoint a designated member of staff with an e-safety role. This may be linked to a member of staff with a child protection role.
- The e-safety policy and its implementation will be reviewed annually.

The school's e-safety policy should be 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.

4.2 Teaching and learning

4.2.1 Why is internet use important?

Discussion: *The rapid developments in electronic communications are having many effects, some profound, on society. Only ten years ago we were asking whether the internet should be used in all schools. Now every pupil is younger than the World Wide Web and many use it more than their teachers. Nevertheless it is important to state what we are trying to achieve in education through ICT and internet use.*

Possible statements:

- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Pupils use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

4.2.2 How does internet use benefit education?

Discussion: *The Welsh Government (WG) has instigated a programme to provide broadband connectivity to the internet via the Lifelong Learning Network Wales (LLNW) and through their document A Learning Country have identified the benefits to be gained through the appropriate use of the internet.*

Possible statements:

Benefits of using the internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the Lifelong Learning Network Wales which connects all schools in Wales;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the Authority and Welsh Government;
- access to learning wherever and whenever convenient.

4.2.3 How can internet use enhance learning?

Discussion: *Increased computer numbers or improved internet access may be provided but learning outcomes must also be addressed. Developing effective practice in internet use for teaching and learning is essential. Librarians and teachers can help pupils to learn how to distil the meaning from the mass of information provided by the internet.*

Often the quantity of information is overwhelming and staff may guide pupils to appropriate websites, or teach search skills. Offering younger pupils a few good sites is often more effective than an internet search. Above all pupils need to learn to evaluate everything they read and to refine their own publishing and communications with others via the internet.

Possible statements:

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be given guidance on what internet use is acceptable and what is not and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.2.4 How will pupils learn how to evaluate internet content?

Discussion: *The spreading of malicious rumour has occurred for thousands of years and information received via the internet, email or text message requires good information handling skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read. In a perfect world, inappropriate material would not be visible to pupils using the internet, but this is not easy to achieve and cannot be guaranteed. It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. More often, pupils will be judging reasonable material but will need to select relevant sections.*

Pupils should be taught research techniques including the use of subject catalogues and search engines and be encouraged to question the validity, currency and origins of information. Key information handling skills include establishing the author's name, date of revision and whether others link to the site. Pupils should compare web material with other sources.

Access to sensitive sites, for example those that record the Holocaust or sites connected to PSE issues, may be required for the duration of a specific educational activity by supervised pupils of appropriate age. The County's filtering system (currently RM) can provide temporary access to specific sites, which a teacher considers necessary for a particular purpose.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

Possible statements:

- The school will ensure that the copying and subsequent use of internet derived materials by staff and pupils complies with copyright law.

The following statements require adaptation according to the pupils' age:

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

4.3 Managing Information Systems

4.3.1 How will information systems security be maintained?

Discussion: *It is important to review the security of the whole system from user to internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.*

ICT security is a complex matter and cannot be dealt with adequately in this document. A number of agencies can advise on security, including Becta. Your policy can also be informed by the Pembrokeshire IT security policy.

Local Area Network security issues include:

- *Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.*

- *Users must take responsibility for their network use. For Pembrokeshire County Council staff, flouting electronic use policy is regarded as a matter for disciplinary proceedings, that could ultimately lead to dismissal.*

- *Workstations should be secured against user mistakes and deliberate actions.*

- *Servers must be located securely and physical access restricted.*

- *The server operating system must be secured and kept up to date.*

- *Virus protection for the whole network must be installed and current.*

- *Access by wireless devices must be proactively managed.*

Wide Area Network (WAN) security issues include:

- *All internet connections should be arranged via the County Network to provide an appropriate level of security and safety.*

- *Decisions on WAN security are made on a partnership basis between school and Pembrokeshire County Council. Where external access is provided to school-based systems, schools must ensure that systems are updated to avoid compromising network security.*

Wireless Networking security and safety issues

Wireless Networking (also known as WiFi) is a technology that allows networks to be created without installing cabling.

The number of wireless access points (WAP) in Pembrokeshire schools is increasing. WAP present an increased risk to the integrity of the individual school network and that of the Pembrokeshire Schools' internet service.

Safety concerns surrounding the technology have prompted a call for more research to be conducted by central government. Pembrokeshire County Council's Education Scrutiny Committee has also discussed the matter a Code of Practice document will be produced by the Authority to provide schools with additional guidance on the use of wireless technology. For further information on this document, or to discuss the use of wireless technology in your school, please contact: Adryan Jones, Health & Safety Advisor for Schools (01267 224765).

Possible statements:

- The security of the school information systems will be reviewed regularly.

- Virus protection will be updated regularly.

- Backup strategies (including off-line and off-site requirements) will be considered and matched to the disaster recovery requirements of the school.

- Security strategies will be discussed with Pembrokeshire County Council where appropriate.

- The school will work closely with Pembrokeshire County Council to ensure e-safety and integrity of any wireless system used or installed in school.

- Personal data sent over the internet will be encrypted or otherwise secured.

- Portable media may not be used without specific permission followed by a virus check.

- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.

- Files held on the school's network will be regularly checked.

- The ICT co-ordinator / network manager will review system capacity regularly.

4.3.2 How will email be managed?

Discussion: *Email is a useful means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools in neighbouring villages and in different continents can be created.*

The implications of e-mail use for the school and pupils need to be thought through and appropriate e-safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils. Once email is available it is difficult to control. The County's webmail system for primary schools offers the possibility to limit email communication to addresses in the school.

In the school context, email should not be considered private and most schools and many firms reserve the right to monitor email.

Pupils should not be identifiable from an email address. For primary schools, whole-class or project email addresses, linked to (and moderated by) a specific member of staff, are easy to use and monitor. Many teenagers have their own email accounts, such as the web-based Hotmail, which they use widely outside school. Most schools ban access to external web-based email, particularly as anonymous identities such as jvj444@mailhost.com make monitoring difficult. Strategies include limiting pupils to email accounts on the school domain or restricting email traffic to the school domain.

Spam, phishing and virus attachment can make email dangerous. The Pembrokeshire County Council mail gateways use Mailscanner to stop unsuitable mail.

Possible statements:

- Pupils may only use approved email accounts within school.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Whole-class or group email addresses, moderated by a teacher, should be used in primary schools.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and may be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

4.3.3 How will published content be managed?

Discussion: *Many schools have created websites that inspire pupils to publish work of a high standard. Websites can celebrate pupils' work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.*

Publication of information should be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or on a secure part of the website which requires authentication.

Possible statements:

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Email addresses should be published carefully, to avoid spam harvesting.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

4.3.4 Can pupil's images or work be published?

Discussion: *Still and moving images and sounds add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Sadly, although common in newspapers, the publishing of pupils' names with their images is not acceptable. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.*

Images of a pupil should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs once per year, other schools ask at the time of use.

Possible statements:

- Images that include pupils will be selected carefully. Associated texts should not enable individual pupils to be clearly identified.
- Pupils' names will not be used anywhere on the website, in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents.

Please see the Becta site, "use of photographic images of children" and the Pembrokeshire Portal e-safety resources.

4.3.5 How will social networking and personal publishing be managed?

Discussion: *Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.*

Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, Facebook, Windows Live Spaces, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Possible statements:

- 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 should ensure that the staff guidelines for the use of mobile phones, email and social networking outlined in the School Staff Electronic Communication and Social Media Policy (in Section 5.0) are adopted as part of the school's internet safety policy or as a separate acceptable use policy for staff.

- 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.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.

- 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 a space has been setup without a password and others are invited to see the bully's comments.

4.3.6 How will filtering be managed?

Discussion: *Levels of Internet access and supervision will vary according to the pupil's age and experience. Internet access should be designed for student use, but cater for all members of the school community as far as safely possible. Older secondary pupils, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions adapted temporarily, where practically possible.*

The technical strategies being developed to restrict access to inappropriate material fall into several overlapping types (commonly described as filtering):

- *Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.*

- *A walled-garden or "allow-list" restricts access to a list of approved sites. Such lists inevitably limit pupils' access to a narrow range of information.*

- *Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.*

- *Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.*

- *Access monitoring records the internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.*

Pembrokeshire County Council currently uses RM Safetynet in primary and secondary schools. This is an industry-standard system used by a many educational institutions around the world.

Secondary schools have their own filtering server and manage their own filtering policy to supplement the core list of banned sites delivered from the central Pembrokeshire system.

Possible statements:

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 will be logged.
- Internet use will be randomly monitored to ensure compliance with school policy.
- 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 disciplinary policy.
- Secondary schools manage the configuration of their filtering. This task requires both educational and technical experience.
- 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.

Internet filtering in Pembrokeshire

Filtering in Pembrokeshire is currently based on the RM Safetynet system and, from September 2014, this will 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.

In the secondary school environment, RM Safetynet offers three possible profiles for each user (in all cases, access is logged for a set period of time):

- **Walledgarden(whitelist). Users are only allowed to visit sites expressly 'allowed' by the school.**
- **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. E-safety officers within secondary schools should be familiar with these facilities; advice and assistance is available from Pembrokeshire IT Consultants.

4.3.7 How will videoconferencing be managed?

Discussion: *Videoconferencing enables users to see and hear each other between different locations. It is a 'real time' interactive technology and has many uses in education.*

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures. The videoconferencing equipment uses a 'network' to communicate with the other site.

Videoconferencing generally uses IP networks. All modern standards-based videoconferencing systems will connect over IP. However, videoconferencing over the internet, even with a broadband connection, can be unpredictable since it is a shared network and quality of service cannot be controlled. Schools using the internet for videoconferencing should be aware that it is not managed by a single responsible agency and that there is no inherent security.

Schools with full Lifelong Learning Network Wales broadband are connected through the Pembrokeshire Schools' Network and have access to JVCS to enable schools to communicate with other external locations. Multipoint Control Units enable several schools to communicate at one time, for instance with several video streams each in a screen window.

Possible statements:

The equipment and network:

- IP videoconferencing should use the Pembrokeshire Schools' network.
- All videoconferencing equipment in the classroom must be switched off when not in use.
- Equipment connected to lifelong Learning Network Wales should use the national E.164 numbering system.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school website.
- The equipment must be secure and if necessary locked away when not in use.

School videoconferencing equipment should not be taken off school premises without permission.

Users:

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and guardians should agree for their children to take part in videoconferences.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key members of staff should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content:

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.

- Recorded material shall be stored securely.

- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

4.3.8. How can emerging technologies be managed?

Discussion: *Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. The safest approach is to deny access until a risk assessment has been completed and safety demonstrated.*

Virtual classrooms and virtual communities widen the geographical boundaries of learning. New approaches such as mentoring and parent access to assessment scores are being investigated. E-safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Facebook. The registering of individuals to establish and maintain validated electronic identities is an important part of the process.

New applications are continually being developed based on the internet, the mobile phone network, wireless or infrared connections. Users can be mobile using a phone with wireless internet access.

Schools should keep up to date with new technologies, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. For instance text messaging via mobile phones is a frequent activity for many pupils. The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive text messages should be dealt with under the school bullying policy.

Possible statements:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy on use in school.

- Staff will be issued with a school phone where contact with pupils is required.

4.3.9 How should personal data be protected?

Discussion: *The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation who processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.*

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal

duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- *Processed fairly and lawfully*
- *Processed for specified purposes*
- *Adequate, relevant and not excessive*
- *Accurate and up-to-date*
- *Held no longer than is necessary*
- *Processed in line with individuals rights*
- *Kept secure*
- *Transferred only to other countries with suitable security measures.*

Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

For advice and guidance relating to a contravention of the Act, contact John Roberts the county's Data Protection Officer:

John Roberts
County Hall
Haverfordwest
SA61 1TP
01437 764551

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/

Possible statement:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4.4 Policy Decisions

4.4.1 How will internet access be authorised?

Discussion: *The school should allocate internet access for staff and pupils on the basis of educational need. It should be clear who has internet access and who has not. Authorisation is generally on an individual basis in a secondary school. In a primary school, where pupil usage is fully supervised, all pupils in a class could be authorised as a group. As most pupils will be granted internet access, it may be easier to manage lists of those who are denied access. Parental permission will be required in all cases - a task that can be organised as part of the Home School Agreement.*

Possible statements:

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Acceptable Use Policy' before using any school ICT resource.
- At Key Stage 1&2, access to the internet will be with adult support and demonstration with directly supervised access to specific, approved online materials.
- Secondary students must apply for internet access individually by agreeing to comply with e-safety rules.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised internet access (an example letter for primary schools is available).

4.4.2 How will risks be assessed?

Discussion: *As the quantity and breadth of information available through the internet continues to grow it is not possible to guard against every undesirable situation. It is wise to include a disclaimer, examples of which are given in the statements below.*

Possible statements:

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Pembrokeshire County Council can accept liability for the material accessed, or any consequences resulting from internet use.

- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risks will be reviewed regularly.

4.4.3 How will e-safety complaints be handled?

Discussion: *Parents, teachers and pupils should know how to submit a complaint. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school.*
A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the member of staff with responsibility for Child Protection issues or e-safety responsibility and the head teacher. Any illegal activity should be discussed with the local Police Public Protection Unit.

See also section 2: Response to an incident of concern

Possible statements:

- Complaints of internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the headteacher.

- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.

- Discussions will be held with the Police Public Protection Unit to establish procedures for handling potentially illegal issues.

- Sanctions within the school discipline policy include:

    - interview/counselling by the head of year;
    - informing parents or carers;
    - removal of Internet or computer access for a period.

4.4.4 How is the internet used across the community?

Discussion: *Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library, youth club, adult education centre, village hall, supermarket or cyber café.*

In community internet access there is a fine balance to be achieved in ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material. Each organisation is responsible for developing access appropriate to its own client groups and pupils may find variations in the rules. Although policies and practices may differ, community partners adhere to the same laws as schools. Staff may wish to exchange views and compare policies with others in the community.

Possible statements:

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

4.5 Communications Policy

4.5.1 How will the policy be introduced to pupils?

Discussion: *Many pupils are very familiar with mobile phone and internet use and culture and it is considered good practice to involve them in designing the school e-safety policy, ideally through the school council. As pupils' perceptions of the risks will vary, the e-safety rules may need to be explained or discussed.*

Pembrokeshire County Council has produced examples of posters with the e-safety rules that are posted on the Pembrokeshire Portal. A poster in every room with a computer will remind pupils of the e-safety rules at the point of use.

The suggested Home School Agreement form should be attached to a copy of the e-safety rules appropriate to the age of the pupil.

Useful e-safety programmes include those provided by:

- Thinkuknow: currently available for primary & secondary pupils. (www.thinkuknow.co.uk/)
- Childline / NCH / Wisekids
- CBBC's Stay Safe Guide: www.bbc.co.uk/cbbc/topics/stay-safe

Possible statements:

- E-safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and internet use will be monitored.
- An e-safety programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
- Guidelines in responsible and safe use should precede internet access.
- An e-safety module will be included in the PSE or ICT programmes covering both school and home use.

4.5.2 How will the policy be discussed with staff?

Discussion: *It is important that all staff feel confident to use new technologies in teaching. The school's e-safety policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation.*

Staff must understand that the rules for information systems misuse for Pembrokeshire employees are

quite specific. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, caretaker, governors and learning support assistants or helpers should be included in appropriate awareness raising and training. Induction of new staff should include a discussion of the school's e-safety policy.

Possible statements:

- All staff will be given the school e-safety policy and its application and importance explained.
- Staff should be aware that internet traffic can be monitored and traced. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible internet use and on the school e-safety policy will be provided.

4.5.3 How will parents' support be enlisted?

Discussion: *Internet use in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the internet. The school may be able to help parents plan appropriate supervised use of the internet at home.*

Possible statements:

- Parents' attention will be drawn to the school's e-safety policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- Interested parents will be referred to organisations listed in section 7.0 - e-Safety Contacts and References.

5.0 School Staff Electronic Communication and Social Media Policy

5.1 Introduction

This policy is provided to protect pupils and ensure that staff are working safely when using electronic communication and social media.

Electronic communications equipment includes (but may not be limited to) telephone, fax, voicemail, computer, laptops, tablets, mobile phones (all types), photocopiers, digital cameras, web cameras, videos and palm-held equipment.

Types of communication can include (but may not be limited to) internet, phone calls, email, text messaging, multimedia messaging, transmission of photographs and moving pictures, contact via websites and social network sites, blogging, wikis, contact via web cameras and internet phones.

Staff should sign the Acceptable Use Policy to show they have understood and accept the contents of this document.

Failure to follow any aspect of this guidance (either deliberately or accidentally) could lead to disciplinary action in accordance with the school's disciplinary policy.

5.2 The internet in school

The internet is a valuable work resource, which enriches teaching and learning. In school hours staff are expected to restrict internet access to work related activities. Reasonable personal use may be permitted outside recorded working time (for example at lunchtime).

Staff must not use electronic equipment for any form of illegal activity, e.g. downloading copyright material, introducing viruses, hacking into other computers, viewing or downloading pornographic, obscene, offensive or any other inappropriate material from any source; transmitting or storing such material on a computer. Criminal proceedings may result if the equipment used for illegal activity is personal or school owned.

Action you must take if you inadvertently access inappropriate material. Anyone inadvertently accessing inappropriate material should immediately inform the headteacher or e-safety officer in school and ensure that the incident is recorded.

5.3 Email

All work-related emails should be written using a school email address. School email should be regarded as an official communication. Emails should be written in the same professional tone and text as any other form of official school communication. Email is governed by the same rules which cover all home-school correspondence.

School email accounts must not be used to send, store or circulate personal email.

The sending of abusive or other offensive email is forbidden and may be considered a criminal act. Bear in mind that emails may be submitted as evidence in legal proceedings and that email discussions with third parties can constitute a legally binding contract.

Email attachments should be opened with care unless you have absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.

An individual should not access the email of another individual within the school without express permission and a clear understanding of the reason for the proxy access. However, staff should be aware that school email accounts may be accessed by other school staff for monitoring or management purposes.

Action you must take if in receipt of inappropriate emails

It is impossible to control what information is sent to a member of staff by email. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the receiver to report immediately, and in writing, to the e-safety officer in school (or the head teacher). Never send a reply.

Keep a printed copy of the email as evidence. Ensure that the sender's information is also recorded as their email service provider may take action.

5.4 Online social communication (such as social networks, blogs)

Many staff and students use the computer for social communication outside school (e.g Facebook, Twitter). Staff should not use school facilities to access or update personal social networks. Staff should be aware that is it a breach of Pembrokeshire County Council policy to add students, or friends of students as 'friends' on their social network site.

Comments made on social networks or blogs should not relate to or identify the school, staff or pupils as this could result in disciplinary action.It is also important that photographs and descriptions of activities in the personal life of staff do not adversely affect the professional reputation of staff or the school. Staff should be aware that even if they have used the privacy settings, they may not be able to prevent material becoming public from 'friends' sites.

It is recognised that online social communications tools, such as blogs and Wikis, have a potentially useful role in schools – such as on school websites, learning journals, celebrating good work, sharing information and facilitating collaboration. Where pupils and their families are sharing these tools with staff in school, it is important that this should always be through a school based provision, such as the Pembrokeshire Portal or Welsh Government Hwb, using a school log-in where all communication is open and transparent.

If staff keep a personal blog the content must maintain acceptable professional standards. Any inappropriate use may lead to disciplinary action in accordance with school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school or Pembrokeshire County Council.

Schools are vulnerable to material being posted about them online and all staff should be aware of the need to report this should they become aware of anything bringing the school into disrepute. Schools should regularly check, using a search engine, to see if any such material has been posted.

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or your school:

Secure and preserve any evidence. For example note the web address (URL) or take a screen shot or copy and print the screen

Report immediately to your line manager or head teacher, who should then report it to the Police.

If appropriate and you are advised to do so, contact the uploader of the material or the Internet Service Provider/ site administrator and ask for the material to be removed.

All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or staff member then the school have a responsibility to deal with it.

5.5 Real time online communication (e.g. texting, using web cameras, chat, mobile phone)

The ability to communicate in real time using the computer and other electronic devices (such as mobile phones) makes these an excellent tool for a range of educational purposes. However staff should

take the same level of care with these tools as they would if working in a face to face situation with a student or group of students. Access should always be through a school created account, never a personal account and it should be focused on a clearly specified educational objective.

There are likely to be times when this kind of activity will happen outside normal school hours and off the school premises. In this situation it should always be carried out with the full knowledge and agreement of a line manager. Staff should be aware that they must remain focused on the educational purpose of the communication and never allow it to become a social exchange.

Staff should also agree to specific times for availability and only allow contact during these times, to protect their personal time. When a web camera is used it should have a clear purpose. Staff should be aware of the ability of meetings of this kind to be recorded without their knowledge. However they may wish to use this function for their own security, as long as all parties are informed that recording is taking place.

Staff must protect their privacy by never allowing pupils or parents to obtain their contact details such as a mobile phone number or login details. Cyber-bullying of staff by pupils is very common by mobile phone or email.

Action you must take if an incident occurs:

Report immediately and in writing to your line manager.

Don't reply to abusive or worrying text or video messages.

Don't delete messages. Keep them for evidence.

Use 1471 to try and obtain the number if you can. Most calls can be traced.

Report it to your phone provider and/or request a change of number

Technical staff may also be able to help you to find or preserve evidence e.g. logs of the call.

5.6 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
- contain inappropriate comments which could cause offence or harassment on the grounds of gender, 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.

5.7 Monitoring and privacy

The school's email and internet facilities are business systems, owned by the school. The school therefore reserves the right to monitor all use of the internet and of the school's ICT systems.

Usage will be monitored to ensure that the systems are being employed primarily for business and educational reasons, that there is no harassment or defamation taking place and that employees are not entering into illegal transactions. Electronic equipment on the school site may be searched and examined.

Staff need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

Email, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used primarily for business and educational reason. To ensure this, monitoring can be carried out on a regular basis. School managers have proxy access to all the school's communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for holiday, illness or other reasons.

Any material stored on the school's network or being circulated via the school's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without an employee's knowledge can be carried out on internal email systems, or information stored on a server. It is permitted to intercept communications in this way so the council can ensure its systems are being used properly in accordance with council policies and are working correctly.

5.8 Breaches and sanctions

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.

5.9 Good practice guidance for school staff

Pay close attention to the list of misuses in section 3 because this list is for your protection and clarifies how possible disciplinary action can be avoided.

In communications with pupils and parents, never give out personal information which identifies your home address, phone number, mobile phone number or personal email address. Once such information is known you are open to harassment through unwanted phone calls, text messages and emails.

Protect your social network site by using the correct privacy settings. Make sure that personal information cannot be seen fromthe links to your friends' sites.

Do not accept pupils as friends on your personal social network site. If at all possible do not include parents as friends.

Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.

Always keep a copy of email communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of telephone conversations.

If your school laptop is used outside school for non-school activities then set up a different user account to ensure that personal or confidential data is protected. Use a strong password to protect the school laptop from unauthorised access.

Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Turn it off, log off and set up a password-protected screen saver to prevent unauthorised access.

Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail as you will then be held responsible for their online activity.

Always use the school's digital camera or video camera for taking school related pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.

The use of hand held walkie talkies is increasing in schools. Staff using this equipment should speak professionally and respect confidentiality. Be aware that the message could be overheard at either end.

If you are using school electronic equipment off site then take the same level of care as you would in school. A digital camera taken off site should not be returned to school with personal photographs on it.

It is not recommended that personal financial transactions are made on school equipment as information may become accessible to pupils.

Observe sensible precautions when taking photographs which may include pupils: always obtain students and/or parental permission and make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school web site or VLE. (Refer to school policy for further guidance on this issue.)

Report immediately, and in writing, to the designated person in school (or your head teacher) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

5.10 Expectations of the school

In order to ensure safe practice for staff, the school should:

Make it clear that the school will enforce policies to protect staff and pupils from malicious use of mobile phones, in particular the use of camera and video functions on phones.

Ensure that the school's policy and procedures for home-school communication are shared with all staff. Establish whole school systems for: storing emails, dealing with inappropriate messages and breaches of security.

Provide all staff with a personal email address - e.g. Education Portal e-mail - to be used for all school-related communications, to be used by every member of staff.

Establish a clear school policy for monitoring use of the school's electronic equipment by staff, including procedures for accessing email and files when staff are absent due to holiday, illness, etc.

Provide digital cameras and mobile phones which can be borrowed by staff as required for all school-related work.

Provide a safe learning environment, such as the HWB All Wales Learning Platform, for electronic communications with pupils

Ensure there are established systems for reporting unwanted or accidental electronic communications and that staff know who is the correct person to report any issues to. Ensure these are correctly recorded. Treat such incidents seriously.

Create procedures to regularly check the schools presence on the web to ensure material detrimental to the school is identified quickly.

6.0 Supporting Materials and Acceptable User Policies

6.0 Supporting Materials

A full range of supporting materials are available through the e-safety resources area on the Pembrokeshire Portal:

www.pgfl.org.uk/portal/cd/widercurriculum/ISafeSite/Pages/Home.aspx

Included below are the Acceptable Use Policies and model letters to parents. These policies have been designed so that you can copy and paste the text into official school documents and add the school name and logo if required. These are also available as individual documents on the Pembrokeshire Portal.

6.1 Acceptable Use Policy for School Staff

I confirm that I have read and understood the Pembrokeshire County Council Electronic Communications and Social Media Guidance for Staff policy and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document.

In particular:

- Any content I post online (including outside school time) or send in an email will be professional and responsible and maintain the reputation of the school
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents
- If I use any form of electronic communication for contacting pupils or parents it will only be via the school's accredited system
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager
- I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils
- Taking photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities
- I will take all reasonable steps to ensure e-safety and security of school IT equipment which I take off site and will remove anything of a personal nature before it is returned to school
- I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded

I confirm I have read the Pembrokeshire County Council Electronic Communications and Social Media Guidance for Staff and will implement the guidelines indicated.

In particular:

- Confidential school information, pupil information or data which I use will only be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended
- I understand that I have the same obligation to protect school data when working on a computer outside school
- I will report immediately any accidental loss of confidential information so that appropriate action can be taken

I understand that the school may monitor or check my use of IT equipment and electronic communications.

I understand that by not following these rules I may be subject to the School's disciplinary procedures.

Name .....

Signed .....

Date .....

6.2 Acceptable Use Policy for temporary or supply staff and visitors to school

As a visitor to the school I recognise that it is my responsibility to follow school e-safety procedures and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all electronic communication equipment provided by the school, and any personal devices which I bring into in school, in a responsible manner and in accordance with the following guidelines :

- I will only use the school network for the purpose I have been given access, related to the work I am completing in the school
- I will not use a personal computer I have brought into school for any activity which might be considered inappropriate in the school
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school or the pupils concerned
- I will not give my personal contact details such as email address, mobile phone number, social media details to any pupil or parent in the school. Contact will always be through a school approved route. I will not arrange to video conference or use a web camera with pupils unless specific permission is given
- I will take all reasonable steps to ensure e-safety and security of school IT equipment, including ensuring that any personal devices or memory devices I use are fully virus protected and that protection is kept up to date
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded
- If I have access to any confidential school information, pupil information or data it will only be removed from the school site with permission and if so, it will be carried on a device which is encrypted or protected with a strong password
- I will report immediately any accidental loss of confidential information to a senior member of staff so that appropriate action can be taken
- I understand that I have a duty of care to ensure that students in school use all forms of electronic equipment and devices safely and should report any inappropriate usage to a senior member of staff
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any Internet sites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

I understand that by not following these rules I may be subject to the disciplinary procedures.

Name .....

Signed .....

Date .....

6.3 Acceptable Use Policy for community users of school computers

As a user of the school's computers I recognise that it is my responsibility to follow school procedures for the safe use of computers and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all means of electronic communication equipment belonging to the school and any personal devices which I bring into school in a responsible manner and in accordance with the following guidelines :

- I will only use the school computers for purposes related to the work I am completing in the school
- I will not use a personal device I have brought into school for any activity which might be considered inappropriate in a school
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school and the pupils
- I will not give any personal contact details such as email address, mobile phone number or social media details to any pupil in the school. I will not arrange to video conference or use a web camera with pupils unless specific permission is given by the school
- I will take all reasonable steps to ensure e-safety and security of school IT equipment, including ensuring that any personal devices or memory devices are fully virus protected and that protection is kept up to date
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

I understand that by not following these rules my use of school facilities may be withdrawn.

Name .....

Signed .....

Date .....

6.4 Acceptable Use Policy for Secondary Students in schools

I understand that use of the Internet and electronic communication is granted to me as a privilege, in return for my acceptance of this agreement. Any misuse on my part may result in loss of that privilege and other sanctions being taken. This also applies to any activity undertaken outside school which contravenes the acceptable use rules of the school.

All online activity will be appropriate to:

- ensure e-safety and security of the school system
- ensure respect for all members of the community
- maintain the reputation of the school

In particular this means:

- I will only access the school IT system and internet via my authorised account and password, which I will not make available to others
- I will ensure that I do not wilfully damage the system by means of malicious code (e.g. virus infections, malware etc), hacking or physical tampering
- Language which I use in electronic communication will be appropriate and suitable, as for all school work
- I will respect copyright of all materials
- I will not wilfully interfere with and /or delete another person's work files
- I will not send or forward messages, publish or create material which is offensive, hurtful or otherwise upsetting to another person. Nor will I post anonymous messages or forward chain letters
- I will not use a mobile phone, camera or other electronic device to take, publish or circulate pictures or videos of anyone without their permission

In addition I understand that:

- Use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is forbidden and may constitute a criminal offence
- Guidelines for safe use of the Internet must be followed and I will report any materials or conduct which I feel is unacceptable
- The school reserves the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary to report anything which may constitute a criminal offence.

Name .....

Signed .....

Date .....

6.5 Acceptable Use Policy for Primary Pupils in school.

- I will take care when using the school IT equipment and use it responsibly
- I will keep my password and login details private unless required to share with a trusted adult
- I will inform an adult if I see or receive any unpleasant material or messages
- I will not interfere with anyone else's passwords, logins, settings or files on the computer
- I will be careful when downloading material from the internet or using material I have brought into school because I understand the risks from virus infections
- Any work I upload to the internet will be my own
- I know I need permission to take someone's photograph or to video them
- Any messages I post online or send in an email will be polite and responsible
- I will not send or forward messages or create material which is deliberately intended to cause upset to other people
- I know I must take care about giving away my personal information and making contact with people I do not know using the internet
- I understand that the school may check my use of IT and contact my parent/carer if they are concerned about my e-safety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or access the internet for a period of time and that this may apply even if the activity was done outside school.

Pupil Name .....

Signed .....

Date .....

6.6 Acceptable Use Policy for Foundation Phase Pupils

- I will take care when using the school IT equipment and use it properly
- I will only share my password or login details with trusted adults
- I will tell an adult if I see anything which upsets me
- I will only take a photograph or video of someone if they say it is alright
- Any messages I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a period of time, even if it was done outside school

Pupil Name .....

Signed .....

Date .....

6.7 Letter for Parents to Accompany Pupil AUP Forms

Dear Parents

Safe use of the internet and email in school

As part of the national curriculum pupils use computers in school to access the internet and to send email. Teaching pupils about safe use of these facilities is included as part of the curriculum. Your child will be introduced to e-safety in a planned and progressive way through school to help them understand how to keep themselves safe when using the internet and other electronic devices. We will ensure that safe use is always included when new activities are introduced to pupils.

As part of our commitment to their safety we always ensure that access to the internet has a valuable educational purpose and is supervised. Internet access is provided by Pembrokeshire County Council through a filtered system which prevents access to the majority of undesirable material. However there is always a small chance that undesirable material can get through the filters but we will teach the children what to do should this occur. We will educate pupils to act responsibly on the internet and to understand some of the risks involved.

When pupils use any form of electronic communication, this will always be in a carefully controlled way so that we know who pupils are in contact with

Many children now have access to the internet outside school, some via their mobile phones. You should be aware this offers pupils much more freedom to use the internet and consequently more ready access to material and activities which might be considered unsuitable. Pupils may also use this freedom to make contact with people they do not actually know, although they may consider them their friends, because they make contact with them on a regular basis. Pupils may also use some of these facilities (such as text messaging, cameras on mobile phones or social network sites such as Facebook) to send upsetting messages or publish things about other pupils which could count as bullying.

We will teach pupils about 'cyberbullying' and the danger of making contact with strangers online as part of the curriculum. We want you to know that we take any activity of this kind seriously even if it takes place outside school, as it can be seriously upsetting for the recipient. We would contact you if an issue of this kind were to arise and would ask for your support in dealing with issues.

I enclose a copy of the Acceptable Use Policy that we operate at our school, which your child is expected to follow.

Yours sincerely

Headteacher

6.8 Image and Video Consent Letter and Parental Permission Form

Dear Parents/ Guardians,

Occasionally, we take photographs of the children at our school. We may use these images in our school prospectus or in other printed publications that we produce, in displays and on our website. We may also make video or webcam recordings for our school website, school-to-school conferences, monitoring or other educational use.

We also send images to the news media, or our school may be visited by the media who will take their own photographs or film footage (for example, of a visiting dignitary or other high profile event). Pupils will often appear in these images. The news media may use the images in printed publications (including local or national newspapers), on televised news programmes or on their website. They then store them in their archive. They may also syndicate the photos to other media for possible use, either in printed publications, on websites, or both. When we submit photographs and information to the media, we have no control on when, where, if or how they will be used.

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child.

Conditions of use:

1. This form is valid for the period of time your child attends this school. Images of your child will not be used after this time. Please write to the school if you wish to withdraw consent at any time.

2. Children will not be named in any photograph or video used on our school website.

3. We may use group or class photographs or footage with very general labels e.g. 'science lesson'.

4. The images we take will be of activities that show the school and children in a positive light.

5. Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues.
6. We will only use images of pupils who are suitably dressed.

7. We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.

8. We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers or for any consequences arising from publication.

Please note that websites can be viewed throughout the world and not just in the United Kingdom where UK law applies. In giving your consent you understand that images may be used in printed and electronic form.

To give your consent, please complete the information overleaf and return the form to the school by end of September. We will assume consent is NOT granted if the form is not returned and therefore your child will not be selected to appear in any photo shoots or in our newsletters etc.

Please tick those that apply:

I give permission for my child's image to be taken and used in publicity material for the school, including printed and electronic publications, video and webcam recordings and on websites ☐

I give permission for images of my child to be used by the news media in printed and/or electronic form and stored in their archives. This might include images sent to the news media by the school and images / footage the media may take themselves if invited to the school to cover an event. ☐

I do not want my child's image used in any publicity ☐

I have read and understood the information overleaf.

Name of child:

Current class:

Parent's or carer's signature:

Name (in block capitals)

Date:

7.0 E-safety Contacts and References

System Leader for ICT

Pembrokeshire School Improvement Service,
County Hall, Haverfordwest SA61 1TP
Tel: 01437 764551 / 07867 381354
duncan.whitehurst@pembrokeshire.gov.uk

Pembrokeshire County Council Helpdesk
Help with filtering and network security.
Tel: 01437 775882
hd@pembrokeshre.gov.uk

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

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

Safeguarding in Education Manager
Tel: 01437 776549 / 07979 058827
cheryl.loughlin@pembrokeshire.gov.uk

System Leader Safeguarding in Education
Tel: 01437 775499 / 07917 263366
kathy.youngpowell@pembrokeshire.gov.uk

HWB All Wales Learning Platform e-Safety Zone
www.hwb.wales.gov.uk/Home/Pages/e-safety.aspx

Child Exploitation & Online Protection Centre
www.ceop.gov.uk

Thinkuknow website
www.thinkuknow.co.uk/

South West Grid for Learning
www.swgfl.org.uk/Staying-Safe

UK Safer Internet Centre
www.saferinternet.org.uk

Wise Kids
www.wisekids.org.uk

Internet Watch Foundation
www.iwf.org.uk/

Childline
www.childline.org.uk/

BBC Stay Safe Guide
www.bbc.co.uk/cbbc/topics/stay-safe

Internet Safety Zone
www.internetsafetyzone.com/

Kidsmart
www.kidsmart.org.uk/

NCH – The Children's Charity
www.nch.org.uk/information/

NSPCC
www.nspcc.org.uk/html/home/needadvice/needadvice

Stop Text Bully
www.stoptextbully.com

Virtual Global Taskforce – Report Abuse
www.virtualglobaltaskforce.com/

8.0 Legal Framework

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, youth workers and health professionals fall into this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools may already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission.

The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.

Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

9.0 Acknowledgements

This document has been produced by the Pembrokeshire County Council e-Safety Group in partnership with Carmarthenshire County Council, is based on e-safety guidance published by Naace and includes statements published by East Sussex, Kirklees and Kent County Councils and the South West Grid for Learning.