St David's Church in Wales Primary School

Acceptable Use of ICT Policy

YR EGLWYS YNG NGHYMRU THE CHURCH IN WALES

ST DAVIDS CIW SCHOOL

ACCEPTABLE USE OF ICT

POLICY STATEMENT

To protect the integrity of the School's computer and network services, all staff must adhere to the Code of Practice laid out in this document. Unauthorised or improper use of the computer services, including failure to comply with these guidelines may result in disciplinary action.

Staff should be aware that the Council reserves the right to monitor and check the content and use of its computer services. Audit trails and management reports are kept for most of the Council's computer services, including e-mail, Internet access and security violations.

Also occasional checks are carried out on desktop PC's to audit their content and staff will be expected to co-operate when these checks take place. Any misuse of computer services or unlicensed software must to be reported to the Operational Manager I.C.T. Services or the Operational Manager Audit, who will take any appropriate action necessary.

LEGAL ISSUES ON THE USE OF COMPUTER SERVICES

Staff must comply with all statutory provisions and regulations relating to computer technology. The main ones are:

THE COMPUTER MISUSE ACT, 1990

In essence this Act makes it an offence to access, or try to access, any computer system for which access authorisation has not been given. Thus any attempt to interfere with, or try to bypass, the security controls on a computing system is an offence. Similarly, trying to obtain information, such as other users' passwords, or accessing or modifying files belonging to other people without access authorisation is also an offence. It is also an offence to facilitate unauthorised access by, for example, disclosing an authorised login name/password combination to an unauthorised individual. Such actions could lead to a criminal prosecution.

THE COPYRIGHT, DESIGN AND PATENTS ACT,1988

This Act makes it an offence to copy documentation or software without the permission of the owner of the copyright. It applies to all software in use in the Council. Breaches of this Act can also lead to legal action.

THE DATA PROTECTION ACT, 1998 (see also updated Data Protection Policy)

In general this Act requires that all personal data relating to other living persons with the exception of personal data held by an individual for domestic and recreational purposes should not be stored by any person on a computer system unless the data is suitably registered. The Council's Data Protection Officer should be consulted if the need to store such data arises. The school publishes a 'Fair Processing Notice' that outlines information that is stored and outlines the type of information who it is shared with.

OBSCENE PUBLICATIONS ACT, 1959

Placing material on the Council's computing facilities in such a way that it can be accessed by several people constitutes its publication. Under the Obscene Publications Act and the Criminal Justice Act, it is an offence to publish material that is obscene.

LAWFUL BUSINESS PRACTICE REGULATION WITHIN REGULATION OF INVESTIGATORY POWERS [RIP] ACT 2000

The Act establishes a new legal framework to govern the interception of communication in the course of their transmission on public or private telecoms systems. The Regulations allow business and public authorities to record or monitor communications in the course of their transmission on public or private telecoms systems. The regulations allow business and public authorities to record or monitor communications without the caller's consent in such cases as:

- Ensuring compliance with regulatory or self regulatory rules or guidance
- Gaining routine access to business communications
- Maintaining the effective operation of systems Monitoring standards of service and training
- Detecting the unauthorised use of systems including protecting the network against viruses or hackers
- Combating or investigating fraud or corruption
- Combating crime and the unauthorised use of the systems

THE HUMAN RIGHTS ACT 1998

This Code of Practice has been reviewed to comply with the Human Rights Act 1998. (Many of the points that follow emphasise constraints already covered by the above legislation.)

FREEDOM OF INFORMATION ACT 2000

This provides the public with the right to gain access to ‘recorded’ information held by public bodies. The school produces a ‘Publication Scheme’ that outlines what information is publicly available.

GENERAL ISSUES FOR STAFF

Staff are individually and personally responsible for following published procedures when accessing computer services.

Computer services must not be used for personal use or any activity not authorised as part of your duties. Do not waste computer services - processing time, network capacity, e-mail, printing capacity, etc - with unnecessary activity. For the purposes of this policy, official business includes the use of the equipment for official Trade Union business.

The school liaises with the ICT Technicians to ensure that all curriculum computers, staff laptops and the Admin PC are protected by up-to-date anti-virus software. The software is automatically configured to check CD's, removable drives and e-mail attachments upon ‘start up’ and these settings must not be changed. Even

with this software active, unauthorised disks, removable drives and CD's must not be loaded onto PC's without a virus scan being carried out first. Any viruses detected with this software should still be reported to the I.T. Service Desk. NOTE: No anti-virus software will guarantee full protection, and staff must also follow good working practices. The briefing paper 'Anti-Virus Guidelines' gives more information on virus avoidance.

The Council views any wilful interference or damage to its installed services and desktop PC's as a serious infringement. Staff are asked to take particular note of the following constraints when using IT services:

- Do not load unauthorised software or data files onto Council computers.
  This includes games, screen savers, programs, magazine CD's, obscene, pornographic material or any material which may contain improper language or any distasteful content and images from the Internet or illegal copies of software.
- Do not load programmes or view files [generally on CD Rom] that have been received from external companies before checking with the IT Section.
- Licensed software will be installed by the IT Section, or by authorised personnel, or under contract with 3rd party companies. Unauthorised staff should not attempt to install or re-install licensed software.
- Do not alter the hardware or system configuration of any Council computer or service or connect/disconnect equipment from the Council's network unless authorised to do so by the IT Section.

Software licence disks are usually held with the software cases, however some are held centrally by the IT Section. The ICT Coordinator is responsible for the secure storage of the software.

Staff should not use any computer service, application software or computer hardware unless you have received proper instructions or training.

No computer services, software or computer equipment are to be purchased unless approved by proper procedures and acquired in accordance with financial standing orders. The IT Section maintains a list of all approved equipment and approved EEC compliant suppliers, and these are referred to initially when acquiring computer equipment. All orders comply with Audit Guidelines.

Any requirement for the school to change its computer services or computer equipment that is connected to the Council network(Admin PC) must be coordinated and approved with the IT Section.

SECURITY

All Data Protection guidelines must be adhered to.
Information about Staff, Pupils and Finance is stored for a maximum of 6 years and it must then be deleted from the system by an ICT technician. SIMS access is password protected and only accessible by the Headteacher and Admin Officer.

All images of staff or pupils should also be removed from the systems in this way, unless parent consent for use on the school website, in prospectus or other school documentation has been given.

If parental consent is given, images of pupils accompanied by their first name only can be used on the school website. Any images of staff and pupils will have protection in place to dissuade downloading or copying.

When using the Internet with 'wireless' technology, staff should use a simple encryption system to prevent the copying of data during transmission.

Staff must take all reasonable precautions to maintain the security and integrity of the School's computer services and information files by:

- Outside normal hours, locking away discs containing sensitive information
- Not divulging passwords and account details.
- Not creating any file shares from a PC unless you have authorisation from the Headteacher/ IT Department.
- Only using services you have been given authority to use, and do not use accounts and passwords of other staff.
- Not opening or viewing files that don't belong to them or for which they do not have authorisation to access.
- Not leaving a computer screen unattended with sensitive information on display.
- Not taking equipment for all staff use off-site without documented management authorisation.
- Not removing copies of the School's software and data files from the premises unless specific authorisation has been given.
- Not passing on data storage devices to another organisation, without fully formatting them first or using new devices. (Special programs are available that can access data from erased files. If you don't follow this guidance, then it is possible sensitive data may be inadvertently passed to unauthorised persons.)
- Not using local passwords, for example Microsoft Word file passwords, unless you have authorisation from the I.T. Department.

HEALTH AND SAFETY

Equipment that is found to be faulty must not be used. All portable equipment is tested annually and certified. Electrical systems are checked every 5 years. Defective or suspect equipment must be reported to the Headteacher. Proactive safety checks, such as cleaning the filter on the Data Projector should be carried out according to prompts.

Staff must conform to the Health and Safety at Work Act. (Details can be obtained from Human Resources and Equalities.) A summary can be found in the yellow Health & Safety File in the office.

ICT equipment should be located in well-ventilated areas, avoiding siting where glare from windows or lights could cause eye-strain, avoiding any need for trailing wires or extension leads and near to a carbon dioxide fire extinguisher.

When using laptops or other ICT equipment at home as part of PPA time, staff must adhere to guidelines outlined in the Risk Assessments ie:

- Working at a desk, in suitable light with a suitable chair, with no trailing wires
- Working in a room, free from interruptions from other users of the home
- Not leaving the laptop unattended, in the car or at home where it could be stolen
- Not leaving applications with sensitive information on view or password protected software open whilst unattended

E-MAIL

Use of emails by staff are monitored by both the Headteacher and the Vale of Glamorgan Council. All emails are kept on record at the Council Server.

Many organisations now regard e-mail communications as binding. Make sure you have gone through proper channels before making any commitments for the School.

E-mail must not contain obscene or pornographic material of any description, improper language or any distasteful content, whether the message is internal or external. If you receive any of the aforementioned please contact the Headteacher and the Operational Manager, I.C.T. immediately. Using the E-mail for receiving and subsequent retention, or sending unauthorised, illegal, obscene or pornographic material of any description, improper language or any distasteful content, whether the message is internal or external may result in disciplinary action for Gross Misconduct. Even though you might not find the aforementioned distasteful, many employees would and the Council will not tolerate its existence.

Staff should not open any unsolicited electronic mail and should take precautions to ensure that files are free of viruses etc.

E-mail - both internal and external - can be used as evidence in a court of law.
Do not make comments that could misrepresent Council, or make personal comments that could be interpreted as libellous.

It is also possible to forge an e-mail. Seek authentication for any unusual email that put demands upon School resources, or impacts upon School policy.

No unsolicited commercial or advertising material is to be transmitted and global mail messaging (termed 'spamming') is strongly discouraged unless there is sound business justification.

Sending global e-mail messages can disrupt other services, there are more efficient ways of displaying public messages - such as the Intranet and public bulletin boards. Contact the IT Section if you are unsure of this. Internet e-mail is not secure. There is greater chance of FAX and normal mail being intercepted than e-mail, but the risk is there. Be careful about using external e-mail for sending sensitive information, or data that has

to be protected under the Data Protection Act. If you need to do this regularly, contact the IT section for advice on encryption and other security options.

Mail attachments - e-mail is a convenient facility for moving spreadsheets and electronic documents around the Council's distributed offices. However, large attachments slow down the responses of our on-line services that share the network capacity with e-mail. E-mail attachments will be limited to 10MB, and the IT Section should be contacted if there is a need to exceed this.

E-Mail is only to be used for official purposes [including college work which is supported by the Council as part of the corporate training strategy]. In emergency situations personal e-mail may be permitted after permission has been received from authorised supervisory staff [Headteacher and above]. E-Mail must not be used for private use, eg E-Mailing friends when not official purposes, as this results in time-wasting.

INTERNET

Using the Internet for unauthorised, illegal or obscene or pornographic material of any description, improper language or any distasteful content may result in disciplinary action. Illegal or obscene use could also lead to prosecution. Even though you might not find the aforementioned distasteful, many employees would. Downloading and storage of images/text of this nature will not be tolerated by the School.

The Admin computer uses the proxy server SWALLOW is a filter that blocks access to inappropriate sites and stops viruses or other malicious programmes being downloaded. Any sites containing items that are illegal, defamatory, inaccurate, potentially offensive, pornographic, racist or fascist should be reported to the co-ordinator so that all staff can avoid them.

The Internet must not be used for private use, as this results in time-wasting and may result in disciplinary action. All staff will have access to the Internet, but use will be restricted to research for professional development or exploring and evaluating resources to support teaching and learning. The school Internet is not intended for personal use.

Check copyright before using any material from the Internet. Information from the Web is, in most cases, the intellectual property of whoever originally created it, and is therefore subject to copyright law in the same way as any other publication. Plagiarism is also a misuse of these resources.

GENERAL ISSUES FOR THE WIDER COMMUNITY

Governors, parents, Health Visitors and other Council departments regularly communicate using email or provide information in e-formats to the school. The school will not tolerate abuses in the form of illegal or obscene or pornographic material of any description, improper language, any distasteful content, breaches of copyright or the sharing of sensitive or confidential material.

PUPIL USE

Internet

The school encourages children's **supported** use of the rich information resources available on the Internet, together with the appropriate guidance and instruction in the appropriate use of such resources. On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources.

Children complete the Agreement form which outlines the rules for acceptable use and E Safety. This is monitored by the class teacher.
Any child who uses ICT to disclose information of a Child Protection nature should be treated in the same way as any other disclosure and the headteacher should be informed. (see All Wales Child Protection Procedures)

Pupil use will only be permitted upon submission of permission and agreement forms by parents. The school believes that the benefits to pupils from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access. If access is denied, first parents will be given the opportunity to view these activities in action and explain how the Internet plays an integral part of the curriculum and how the lack of access would disadvantage their child. If consent is still withheld then the child would have to be removed from classrooms when these activities were taking place.

As much as possible, the school's chosen information provider has organised information resources in ways that point pupils to those that have been reviewed and evaluated prior to use. The current ''homepage'' is' Eduweb' an educational website aimed at primary school children's levels of attainment and understanding. While pupils may be able to move beyond those resources to others, they shall be supervised at all times and guided to resources particularly suited to the learning objectives.

However, Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources that are inappropriate for use by children. The Vale Web Filter for Curriculum PC's– "Websense" also blocks access to inappropriate sites and stops viruses or other malicious programmes being downloaded.

It is the responsibility of the supervising teacher to ensure children do not view material containing items that are illegal, defamatory, inaccurate, potentially offensive, pornographic, racist or fascist. Staff must report any accidental access to the ICT Coordinator, who will email the ICT section

ICT equipment

Children are taught the basic safety rules before being allowed independent access to PC's or whiteboard:

Obsessive use of ICT or the Internet is discouraged and all children are motivated to use a broad range of activities.

The IT co-ordinator will ensure that all staff are trained and provide advice on content and appropriate teaching levels consistent with the school's IT programme of study.

MONITORING THE POLICY

The Headteacher is responsible for monitoring all aspects of the policy and refining and regularly up-dating it in regard to new technologies and practice. The Headteacher reports to the Governor with responsibility for ICT on all matters.

Any staff misuse or abuse will be referred to the Disciplinary Committee of the Governing Body and gross misconduct could result in dismissal procedures.

LONG TERM ICT STRATEGY:

IS AN INTEGRAL TOOL FOR MOTIVATING, INFORMING & REPORTING HIGH QUALITY TEACHING & LEARNING

- Continue to monitor children's developmental progress to determine whether IT skills ladders need extending with new technologies
- Introduce email facilities for children
- Establish web-cam links with other church school providers

- All staff confidently use ICT resources that reflect technology used in the wider community to enhance children's learning; assess, monitor & analyse learning; and to record and report children's progress.
  - Ensure new skills ladders form the basis of Excel Spreadsheets to monitor individual progress- merge with SIMs to enable more comprehensive analysis
  - Parents to receive Reports electronically like newsletters or access pupil file via Portal
  - Encourage greater number of consultations/SEN & EBD reviews or updates to be electronically for working parents
  - Use observation time to monitor children's independent use of ICT
  - Ensure Curriculum Area policies reflect provision for ICT

IS USED ACCORDING TO HEALTH & SAFETY REQUIREMENTS AND TEACHES E-SAFETY

- Introduce ICT Parent meeting – training in e-safety issues
- Website to include section of e-safety with links to appropriate parent/children sites

ENABLES EFFECTIVE & SECURE ELECTRONIC ADMINISTRATION & MANAGEMENT FOR THE SMOOTH DAY TO DAY RUNNING OF THE SCHOOL

- Ensure Induction Training includes Acceptable Use of ICT Policy
- Increase use of the "Report" function of the SIMs system when gathering & analysing data by all sanctioned staff

EFFICIENTLY & SECURELY COMMUNICATES INFORMATION ABOUT ALL ASPECTS OF SCHOOL LIFE TO INTERESTED PARTNERS

- Replace main school diary with e-diary
- Staff to have electronic personal organisers with automatic daily link via Portal
- Website to be submitted, which includes information about all aspects of school life and relevant wider community links
- Increase the number of parents who receive ParentMail
- Encourage parents to have e-copies of policies rather than photocopies

SKILLS OF ALL PERSONS INVOLVED WITH THE SCHOOL CONTINUALLY DEVELOP TO ENHANCE THEIR WORK THROUGHOUT THE SCHOOL

- Annual "Audit Staff Skill Needs" to be updated to reflect new technologies.
- Continued training – INSET courses/in-house staff meeting –shadowing-mentoring/ good practice visits using SEG Grant
- Governor induction to include ICT skills
- Introduce ICT Parent meeting – training in e-safety issues

RESOURCES ARE INNOVATIVE AND SUSTAINABLE IN REFLECTING THE DIVERSE NEEDS OF THE WIDER COMMUNITY

- Components of PC's to be upgraded to capacity before replacing – including external hard drives
- Encourage parents to support Tesco Voucher Schemes
- Encourage Industry or Community Link funding/match funding projects for larger items
- Staff awareness new technologies: ICT conferences-BECTA site-Internet – EY magazine reviews
- Link with the community to buy second hand computers enabling us to sustainably improve the schools resources.

- ***ACTIVITIES NURTURE PUPIL'S NATURAL ENTHUSIASM FOR THE SUBJECT AND ENCOURAGE THEM TO UTILISE THEIR SKILLS TO ENHANCE THEIR LEARNING AND PRESENTATION***