

ICT POLICY

1.

PREAMBLE

- 1.1 The Governors and school are fully aware of the benefits of ICT and appreciate fully the need to comprehensively embrace this technology to greater enhance the life chances of all at the school.
- 1.2 The Governors and school are mindful of the potential misuse and harm to which aspects of ICT may lend itself. Consequently, there is a need to carefully manage the use of ICT at school.
- 1.3 For the effective and efficient use of ICT, the considered execution of roles and responsibilities needs to be clarified and explained to all interested parties.
- 1.4 The Governors and school are mindful of the relevant legislation that relates to ICT, namely:-
 - Obscene Publications Act 1959
 - Race Relations Act 1976
 - Copyright Designs and Patents Act 1988
 - Computer Misuse Act 1990
 - Data Protection Act 1998
- 1.5 The Governors and school are further aware of the position of the LEA with respect to the policies, procedures, advice and guidance provided by them:-
 - Freedom of Information Act 2000 – A Guide for Schools
 - ICT Code of Practice (Internet & E-Mail Usage) 2004
 - Internet Access for Schools Policy 2003
 - Safe Use of Images Policy
 - Six Simple Rules for Using Bridgend ICT

2.

POLICY

- 2.1 The policy will ensure safe access to ICT for all at Porthcawl Comprehensive School.
- 2.2 The policy will ensure the school's use of ICT is both legal and complies with the advice and guidance offered by the LEA.
- 2.3 The policy will detail the roles and responsibilities for those who organise, maintain and manage ICT at the school.
- 2.4 The policy will inform and educate both pupils and parents as to what is acceptable and proper use of ICT.

- 2.5 The policy will stipulate precise conditions of usage of ICT at this school. These will involve parents, pupils and staff.
- 2.6 The policy will indicate data back-up procedures and disaster recover procedures.
- 2.7 The policy will aim to allow ICT to enhance and enrich the learning opportunities for all at Porthcawl Comprehensive School.

3. **PROCESS**

- 3.1 The **Governing Body** will oversee, endorse and review the school's ICT Policy document.
- 3.2 The **Headteacher** will:-
- liaise with the Governing Body on the review and development of the ICT Policy;
 - be responsible for the safe and appropriate use of ICT at Porthcawl Comprehensive School;
 - encourage and give a lead as to how ICT will enrich learning experiences at Porthcawl Comprehensive School;
 - manage (through devolvement) the day-to-day organisation of ICT at this school;
 - take reasonable steps to inform parents/carers that at times images of children will be taken and may be used for the newsletter which is posted on the website;
 - communicate with parents/carers to allow them the opportunity to object to any image of their child being included in any materials being developed;
 - seek the express written permission of parents/carers when pupil images are used for direct reasons e.g. school show programme or prospectus;
 - take all reasonable steps to ensure no accompanying text will directly identify an image of a child;
 - ensure that the potential misuse of images of children is a risk understood by all and that all images will be wholly appropriate.
- 3.3 The **Deputy Head** will:-
- be responsible for the strategic development of ICT at the school;
 - assume day-to-day management of ICT in school;
 - liaise with interested parties, i.e. Head of ICT, ICT Technicians etcetera, surrounding ICT issues;
 - have regard for the responsibilities of the Headteacher and will implement these in the day-to-day life of the school, i.e. in supervising production of newsletters etc;
 - will ensure that any request for hard copies of any policy will be made available upon receipt of a signed, written request.

3.4 ***Heads of Department*** will:-

- be responsible for ICT resources deployed within their departments;
- take steps to ensure safe and appropriate use of ICT at departmental level;
- lead and encourage others to enrich learning experiences by developing further the use of ICT in lessons;
- be aware of and implement the school's ICT Policy and associated procedures.

3.5 ***Teachers*** will:-

- be responsible for their ICT equipment and take all reasonable steps to ensure safe and appropriate use of ICT;
- develop materials that use ICT to enrich learning experiences for pupils.

3.6 ***ICT Technicians*** will:-

- carry out routine maintenance on all ICT equipment and software in school;
- carry out repairs as directed;
- ensure the safe and ordered back-up of both the Administration and Curriculum servers;
- provide advice and guidance as required;
- provide routine and regular system up-date information;
- manage the internet provision both internally and externally;
- Ensure the proper use of security codes (see 4.2).

4. **PROCEDURES**

4.1 **Internet Access**

The school operates within the guidelines of the LEA's "***ICT Code of Practice (Internet & E-Mail Usage)***". Appendix 1.

The school has developed an "***Internet Access Policy***". Appendix 2.

The school has adopted a procedure to involve parents and pupils in the safe internet protocol. A record of parental permission and a register of users will be maintained at Porthcawl Comprehensive School. Appendix 3.

4.2 **Password Protection Procedures**

All access to either network will be governed by a hierarchical password system.

All pupil users have a username and password that allows them to access an account on the Curriculum server. Pupils are told to keep their password a secret and not to allow others to know it thus preventing them from accessing one another's accounts.

All teachers have passwords to the Curriculum server. Further encrypted passwords are required by those who access PPMS, Teamware or Sims. In the case of software access passwords staff are encouraged to regularly change both their password and PIN numbers.

Only senior staff and technicians have password access to “maintenance” elements of software and machines are protected by “fortress”.

Passwords will be changed frequently.

4.3 **System/Data Back-Up Procedures**

Curriculum Network

The system uses a weekly tape back-up system in which one of five tapes is overwritten on a weekly basis.

The back-up tapes are stored in a lockable steel cabinet in the ICT Office in P Block.

A daily log of the back-up procedures will be kept by each of the ICT Technicians.

Administration Network

The system is backed up on a two week tape cycle. Tapes are thus overwritten on a two week cycle.

The back-up tapes are stored in school and a copy is taken off-site each evening (ICT Technician).

An annual back-up is made to record student and staff data in ‘P’ and department drives.

Under the terms of a SLA, the LEA remotely backs-up the Admin server on a daily basis.

Software

All purchased (master) copies of software are stored in a lockable steel cabinet in the IT Support room.

4.4 **Virus Control**

The school is aware of the potential danger that virus infection poses to systems and software. To counter this problem, the school has a contract with “NOD32” for anti-virus software. This is a three year contract set to expire in November 2011.

The Curriculum network is set to accept software downloads at 12.00 hrs daily. These downloads cover:-

- Windows 95/98/ME
- Windows 2000/XP/2003
- Windows NT

The up-dating policy is set to check for new versions of the software every 200 minutes.

The Administration network has NOD32 installed on the 25 machines in this network. It is policy and practice to install NOD32 on all laptops, tablet PCs and palm tops.

4.5 **Cyber Bullying/Harassment**

Cyber bullying/harassment is the use of modern ICT applications to deliberately cause distress to a third person. A simple definition of cyber bullying/harassment is "sending or posting of harmful or cruel text or images using the internet or other digital communication devices". The effects upon a victim can be devastating. Any offending material can stay on web sites for years, spread quickly and does not stop at the school gate, entering the victim's personal space. There will be negative effects on the victim's confidence, reputation, credibility, career progression and personal relationships.

The school regards any form of content that is libellous or defamatory in any way as an example of cyber bullying/harassment. It is recognised that cyber bullying/harassment is particularly harmful and has a potentially far-reaching and long-lasting impact upon the victim.

This policy document makes it very clear that any form of cyber bullying/harassment will not be tolerated. Whilst acknowledging the ease of anonymity via the web, the school will make every effort to discover the origin / authorship of any such material.

The school regards such acts as among the highest form of offences. Consequently, any such instance will be dealt with very seriously. Any originator/author/poster of any form of cyber bullying can expect to be dealt with in the most severe manner.

Guidance for parents

There are a number of useful websites that may offer guidance for parents and learners alike.

We recommend you consult:-

www.anti-bullyingnetwork.net

www.childnet.com

www.teachnet.gov.uk