INSPIRE • CHALLENGE • SUCCEED

YSGOL
TREFFYNNON

ICT Policy

Reviewed by:	Progress & Standards Committee
Version:	1
Adopted by FGB on:	1st October 2014
Signed by:	(Chair of Governors)
Next Review:	1st October 2015

ICT Mission Statement

Our vision is for all teachers and learners in Ysgol Treffynnon to become confident users of ICT so that they can develop the skills, knowledge and understanding which enable them to use appropriate ICT resources effectively as powerful tools for teaching & learning.

Introduction

The significance of Information and Communication Technology

Information and communication technology (ICT) prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognise that Information and Communications Technology is an important tool in both the society we live in and in the process of teaching and learning. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with pupils being able to make informed judgements about when and where to use ICT to best effect, and consider its implications for home and work both now and in the future.

This policy document sets out the school's aims, principles and strategies for the delivery of Information and Communication Technology. It will form the basis for the development of ICT in the school over the next five years. This policy was developed in the Autumn term 2010 by the Governors Curriculum Committee. It was amended by the Governor's Curriculum Committee on Tuesday 16th September 2014 ready for submission to the Full Governor's meeting on Wednesday 1st October 2014.

Reference is made to the School's Assessment and Health and Safety policies. Full details of our software and hardware resources and maintenance procedures are included in the staff handbook.

The aims of the School ICT Policy

The overall aim for Information and Communication Technology is to enrich learning for all pupils and to ensure that teachers develop confidence and competence to use Information and Communication Technology in the effective teaching of their subject.

- Information and communication technology offers opportunities for pupils to Develop their ICT capability and understand the importance of information and how to select and prepare it.
- Develop their skills in using hardware and software so as to enable them to manipulate information.

- Develop their ability to apply ICT capability and ICT to support their use of language and communication.
- Explore their attitudes towards ICT, its value for themselves, others and society, and their awareness of its advantages and limitations.
- Develop good Health and Safety attitudes and practice.

The school's curriculum organization

Children arrive in school with variable ICT experiences: the systems are different and sometimes the software is different. We view these prior achievements as an advantage and aim to build on them.

ICT lessons are taught in all Lower School years. In addition ICT Capability will also be delivered within subjects in every year group. The ICT Coordinator, in discussion with Heads of Department, will timetable the use of the school resources to ensure this will happen. We interpret the term 'information communication technology' to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically.

Key Stage 3 ICT

A skills and techniques curriculum from the QCA schemes will be the basis of the ICT curriculum and this will be built upon by applied use in subjects:

- ICT Using ICT Information and Presentation Models: rules and investigations Data: designing structure etc. Processing text and images Control: Input, process and output
- Cross-curricular ICT through English, History, Maths, Geog, RE, Science, Food, D &T, MFL & Cymraeg.

Year 10 OCR Nationals ICT

It is now a statutory requirement that all pupils at Key Stage 4 study for a qualification in ICT. All pupils in the current Year 10 (and then into Year 11) will study for an OCR National Level 2 qualification.

ICT is organised in the school through working within the scheme of work which is based on the National Curriculum programmes of study.

Curriculum Management

The ICT Coordinator will, with the assistance of the School Network Manager, facilitate the use of Information and Communication Technology in the following ways:

- By updating the ICT policy and scheme of work;

- By informing the Governors’ Curriculum Committee of any changes made to the ICT policy as a result of the annual review;
- By ordering/updating resources;
- By providing INSET so that all staff are confident in how to teach the subject and have sufficient subject knowledge;
- By keeping staff abreast of new developments;
- By taking an overview of whole school planning to ensure that opportunities occur for pupils to develop an information and communication technology capability and that progression is taking place;
- By supporting staff in developing pupils' capability;
- By attending appropriate courses to update knowledge of current developments, and by keeping links with the Advisory Team for Information and Communication Technology;
- By contributing to the School Improvement Plan on an annual basis
- By management of the Network Manager if available and communication of problems to the LA support team.
- Making sure all staff understand system for logging faults and use of the Internet/email
- Monitoring the curriculum
- Maintaining records of software licences and their deployment.

Access to ICT

Network access

Staff and students have access to reliable and industry-standard hardware and software in order to use ICT effectively as a teaching and learning resource, and as a working tool for management and administration. Every classroom has at least one PC for staff use.

All staff and student users have access through the school’s Curriculum network to their personal data areas, shared data, applications that are not held locally including LGfL, and the internet.

The Administrative network, which is managed by the Network Manager, allows all staff access to SIMS for electronic student data, timetables and attendance.

Computers for student use

Teaching of core ICT and ICT within subjects is mainly in the four computer suites located across the school site. There is an additional suite to be located in the Design Technology department. An additional small suite is primarily used by Sixth Form students for private study. "Free" slots are can then be booked in any of the suites by any member of staff (www.roombookingsystem.co.uk/holywell) when needed.

A policy of integrating ICT into teaching and learning across the curriculum is reflected in the ongoing provision for the expansion of digital projectors and interactive whiteboards in classrooms. There are now a large number of these in subject areas and it is hoped that this will be expanded on over the next few years such that a digital projector and interactive whiteboard will be installed in every classroom wherever feasible.

Staff issues

All staff are entitled to training to improve their ICT capability and have a responsibility to keep abreast of developments in ICT. The ICT Coordinator, the Network Manager and the County ICT support Unit can be contacted to request support and training in the use of ICT.

Student data

All staff are provided with training in pupil data management information systems (SIMS.net) on request. Subject Leaders and Year Leaders have a responsibility for improving the use of data throughout the school. There is a rolling programme of improving access to, and improving the quality of, staff computers throughout the school.

From September 2008 the school started using electronic registration to improve pupil attendance. Staff register classes every lesson through the PC in each classroom. In the event of technical difficulties, paper registers are taken and sent to reception for collation and entering onto the system as soon as possible. Attendance and lateness is regularly reviewed by Heads of Year and suitable action taken to reduce instances of lateness or truancy.

Line managers identify with staff their ICT training and development needs and inform the School Development Plan. Other staff developments are identified through performance management procedures and any new initiatives that require whole school training.
Staff are expected to use ICT based procedures to book and record CPD.

All staff use online assessment procedures to record and report on student progress.

Inclusion

All pupils, regardless of race or gender, shall have the opportunity to develop ICT capability. The school will promote equal opportunities for computer usage and fairness of distribution of ICT resources. Children with a computer at home are encouraged to use it for educational benefit and parents are offered advice through the acceptable use agreement about what is appropriate.
Efforts are made to ensure that text created at home can be transferred to a classroom computer once a teacher has been notified. The school will monitor the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged. Groupings for computer usage should generally follow the same pattern as for all lessons. It is appropriate to match pairs of equal ability, rather than have a more able ICT users always guide a less able pupil. This generally leads to passivity and dominance. However it is

appropriate to plan to have peer tutors for some lessons where the objectives also enable the more able user to learn by specifically teaching. Positive images of computer use by people of both sexes will be promoted. The school recognises the real advantages of the use of ICT by children with additional learning needs.

Using ICT can:

- address children's individual needs
- increase access to the curriculum
- enhance language skills

Staff should structure their teaching materials to match a learning difficulty. If the situation arises, the school will endeavour to acquire appropriate resources to suit the specific needs of the child.

Recording, assessment and reporting

As the class teacher works through the scheme of work they will record progress against the short-focused tasks where appropriate and assess the children's progress in the integrated task. This assessment will be used to support teaching and learning. Assessment will be based on some, most and further in line with QCA recommendations.

Some evidence is to be kept. This may include a description of the context and an explanation of how the pupils completed the task. Photographs, discussion, saved work on the network and printouts (if any were produced) of differing pupils work. This will be known as a Portfolio of Exemplar Assessments and will accompany the children throughout their time at the school. The ICT teachers at Key Stage 3 and 4 will be expected to meet at least once a year to compare the standards of assessed work. This moderation should be carried out in line with LA, WJEC and WAG advice.

ICT work will be marked in line with the school policy on marking.

For reporting purposes, which will be at the end of Key Stage 3, a level of each pupil's ICT capability will be given. This will be based on the attainment target level descriptions.

Monitoring and review

Monitoring is carried out by the Headteacher (member of senior leadership team) and the ICT coordinator, in the following ways:

- Informal discussion with staff and pupils
- Faculty Reviews
- Observation of ICT displays
- Collection of class ICT files

- Looking at the work in their individual paper files or notebooks
- Classroom observation

There is an annual review of this policy by the ICT coordinator. A major review involving all staff will take place every three years.

Health and Safety/Security

Before being allowed to work in the computer suites all children are made aware of the arrangements if they hear the fire alarm. A copy of the evacuation route and location of fire extinguishers can be found on the wall of the suite. Portable equipment will be checked annually and computers three-yearly under the Electricity at Work Regulation 1989.

Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers. Computer Room Rules are also on display within the ICT room for reference along with specific rules for the use of Internet and E-mail. The school also has a 'Responsible Use of The Internet Policy' document.

The Health and Safety at Work Act (1 January 1993), European Directive deals with requirements for computer positioning and quality of screen. This directive is followed for all administration staff. Whilst this legislation only applies to people at work we seek to provide conditions for all children which meet these requirements.

The school has an alarm system installed throughout. Each computer system has individual security against access to the management system. The files and network system are backed up regularly. The virus checker is updated regularly.

Ysgol Treffynnon has its own website www.holywellhighschool.co.uk. Here school information will be continued to be displayed and shared.

Data Security

As part of the data protection act it is expected that the school must take suitable steps to ensure that sensitive data about students is not lost. Employees of the school must not put sensitive data (which contains information about a pupils address, contact details etc…) onto a removable memory device (such as a USB pen drive). If data is to be placed onto any removable memory device then the data protection officer for the school (Mr I Evans) must be consulted and, if approved, must be suitably encrypted.

Teaching staff may wish to use an “electronic mark book” to record pupil progress. This could be placed onto a removable memory device as long as the pupils were only identified by name. For example, information on birth date must not be included.

Acceptable Use

Ysgol Treffynnon provides access to networked computers to support students' academic work. Our Acceptable Use Policy (which can be seen in Appendix A) is an extension to the School Rules. It includes guidelines for the safe and responsible use of the network and the internet, and identifies those activities which constitute an abuse of our ICT facilities.
In summary, users of the school network are prohibited from:

- logging on to the network with another user's account
- creating or sending offensive or harassing materials to others
- altering the settings of school computers or making other changes which render them unusable by others
- tampering physically with the equipment
- installing software without authorisation
- hacking into unauthorised areas of the network
- accessing inappropriate websites or trying to circumvent the College filtering system
- attempting to spread viruses via the network
- any form of illegal activity, including software and media piracy

Use of WEB 2.0 resources

Students may be encouraged to access the School Moodle site while at home. They may be asked to contribute to wiki’s and forums.

Internet and use of videos

Internet access and videos are planned to enrich and extend learning activities. However, setting poorly structured ‘research’ tasks is shown to be counter-productive. Research tasks should be clearly set out with measurable outcomes. The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies. Although the school offers a safe online environment through filtered internet access we recognise the importance of teaching our students about online safety and their responsibilities when using communication technology.

The use of videos must also be planned and directed. Teachers must ensure correct use of the age-certification. On no account must students watch videos that are above their recommended viewing age. As the school does not possess a licence to show films, DVDs or videos for non-curricular purposes, students are not to watch non-curriculum related films, DVDs or videos in the final week before school holidays

Taking and using images of students

The school has identified three uses for images of students:

1) For administrative purposes. Photographs of students are placed onto SIMS.net to help identify them.
2) For publicity purposes. Photographs of students may be taken and given to the local or national press to illustrate achievements made by them in school.
3) For assessment purposes. Photographs or videos featuring students may be taken as part of the assessment process. These are then sent off to the examination board.

Sustainability

Technical support routines and procedures are continuously reviewed and developed to ensure the sustainability of the network infrastructure, hardware and software.
The whole school asset register provides a continuously-updated audit of hardware that facilitates decisions on repair, replacement and development.
The whole school annual budgetary cycle provides the opportunity to identify maintenance, replacement and development needs for ICT infrastructure, network services, technical support, equipment, and software.

Before being disposed of, all ICT equipment is firstly made safe and removed from the schools register of assets and PAT testing register. Hard drives that have been used in administrative computers and those used in curriculum machines are reformatted to wipe all data and stored for possible reuse. It may be necessary to buy software that will guarantee complete erasure of data. Equipment is then stored in a secure location on site until there is a suitable amount for it to be removed by a registered waste removal company who issue a waste disposal receipt. To facilitate this, the school is registered with the Environment Agency as a Generator of Hazardous Waste.

Copyright and licensing

The school will only allow use of licensed software on the school network and any stand alon machines owned by the school. It is the responsibility of the network manager with assistance from county the the licences on all the network machines is valid. Staff should not load software onto network machines without discussing it with the Network Manager. The school agrees to respect the intellectual ownership of software as defined by the Copyright Designs and Patents Act 1988 and 1991 European software Directive.

Appendix A: Ysgol Treffynnon Acceptable document

The purpose of this policy is to ensure that the safety and privacy of all users is maintained when using the Internet and WWW through the Ysgol Treffynnon computer system. Users are taught to use the facility sensibly and with proper consideration for others.

1. Any images of students will not be labelled with their names and no close up pictures of our students will be available Online.

2. Students and staff should never reveal their personal details, home addresses and telephone numbers, nor those of others, on the web or when in dialogue with other Internet users.

3. All computer accounts (usernames and passwords) are for the use of a single individual, the person for whom the account was approved. Sharing or loaning accounts is strictly prohibited. All actions when an account is in use are the responsibility of the account holder.

4. Use of these facilities to gain unauthorised access to any other account, at this school or any other facility, is expressly prohibited.

5. E-mail addresses are allocated to individual users. All e-mails passing through the school computer system are monitored by County ICT for malicious and/or offensive content, in addition to unsuitable text and images following proper authorisation.

6. Chat room’s and web based e-mail are not to be used by users through the Ysgol Treffynnon computer system. If access is enabled to users, students will not engage in conversation or dialogue with other users on the Internet without permission or supervision from their teacher.

7. The free use of the Internet is not permitted to pupils (except Sixth Form) unless in the presence of a teacher or other adult in school. Downloading of files is restricted to staff.

8. Any students finding themselves uncomfortable or upset by anything they discover on the Internet will report it to a member of staff immediately.

9. A member of staff has the right to check student’s personal disks for viruses and unsuitable material before they will put any work in the users folder on the Ysgol Treffynnon computer system.

10. All Internet access at Ysgol Treffynnon is filtered through a proxy server at County ICT to screen undesirable sites at source.

11. Users must agree not to access unsuitable material or inappropriate websites when using the school computer system. Users must act responsibly and use the Ysgol Treffynnon computer system for course/school related work only.

12. Users must respect copyright laws and not plagiarise work.

13. Ysgol Treffynnon has the authority to disable users, e-mail facilities and Internet access immediately without warning for failure to comply with this policy. The school must be strict in these matters to ensure that any user breaching this agreement is prevented from bringing the school into disrepute and to ensure that the integrity of the school is maintained for the school, its users and staff.

14. Anything published on the Internet using the Ysgol Treffynnon computer system is subject to all applicable UK publishing laws.

15. Users have a duty to report infringements of this code by others to a member of staff.

Appendix B – Safe use of ICT

How will Email be managed?

Electronic mail (email) is simple to use and relatively cheap. The content of electronic mail messages transmitted via FlintNet are checked via software in a process managed by the ICT Unit. However, care needs to be taken that the potential consequences of reading and sending messages, for both the pupil and the school, are appreciated.

Pupils should be made aware of the appropriate actions to take if they receive unwanted interactions by email. Bullying, abuse or harassment by email should be dealt with in the school's anti-bullying policy. Pupils should be advised to guard against giving out personal information at all times.

One of the key considerations is reducing the risk of unsolicited attention put on individual pupils from people outside the school. If individual pupil addresses are used there is a risk of people from outside the school contacting pupils direct. A class/teaching group email addressing system gives complete anonymity to pupils, allows teachers to monitor mail and therefore reduces the risk. Care should be taken if allowing pupils to attach files to email messages.

There are concerns regarding the filtering of emails relating to breaches of individuals rights to privacy etc. Filtering and monitoring is used and details of the approach should be included in the school's Acceptable Use Policy.

Email use is a key concern for schools in terms of safety and management. Parental consent should be obtained for pupils to use email. This should be informed consent with parents having access to the school's Acceptable Use Policy.

With developments of the cloud, it is possible to generate email accounts that are available to staff in school and at home. These mail accounts often come with an online storage facility which allows access to documents and other files from a range of internet capable devices. It should be noted that these types of mail systems aren't backed up, so important files or mail should be copied to another secure location. No sensitive materials or files should be hosted on the cloud without due thought to protecting that data.

How will the school ensure Internet access is appropriate and safe?

Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. The Internet is a new communications medium and staff will need to ensure that access is appropriate to the user. Teachers may expect access to watch YouTube or other video streaming sites as part of everyday teaching activities. Such access brings greater freedom and opportunity but also carries greater responsibility for the teacher to ensure that the content is both educationally suitable and appropriate for pupils to view. Protected access will be required for all pupils. Primary pupils and younger secondary pupils will require highly protected access to the Internet. The oldest secondary pupils, as part of a supervised project, might need to access adult materials, for instance a set novel that includes references to sexuality or racism. Teachers might need to research areas including drugs, medical conditions, bullying or harassment. Systems will soon enable different levels of filtering to be applied by time, location and user.

- *Screens used by pupils will be in public view to staff and pupils in the same group.*
- *Staff will check that the sites selected for pupil use are appropriate to the age and maturity of pupils.*
- *Staff will be responsible for checking that the content of videos streamed or downloaded from YouTube and other video hosting sites are educationally appropriate to the age and maturity of pupils*
- *Senior staff will monitor and regularly review the effectiveness of access strategies for electronic communication.*
- *Access levels will be reviewed as pupils' Internet use expands and their ability to retrieve information develops.*
- *Senior staff will ensure that occasional checks are made on files to monitor compliance with the school's Electronic Communications Acceptable Use Policy.*
- *A range of fully tested approved sites will be made available for pupil use.*
- *If staff or year 12/13 students require less restricted Internet access a separate arrangement will be provided via a specific request, made electronically or in writing, to the ICT Unit by a member of the senior management team.*
- *Links to electronic sources placed on the school web site or VLE will not enable access to any resources/materials not available from within the school.*

- *Inappropriate use that results in contravening the school's Acceptable Use Policy for Electronic Communication and e-Safety may be investigated by staff of the ICT Unit and Council Officers.*

How will complaints be handled?

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 example it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions may be of a minor or potentially significant nature. Sanctions for irresponsible use will be linked to the school's behaviour/disciplinary policy.

Possible statements:

- Responsibility for handling incidents will be given to a senior member of staff.

- Responsibility for handling incidents will be given to a member of the senior management team.

- Responsibility for handling incidents will lie with the Headteacher.

- If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the ICT Unit. The ICT Unit will immediately prevent access to any site considered unsuitable. Where appropriate investigation will be undertaken. Appropriate action will be taken – as defined within the Commitment by Flintshire County Council. As with drugs issues, there may be occasions when the police must be contacted. Where necessary, following discussion with the Headteacher, early contact will be made to establish the legal position and discuss strategies.

- Parents and pupils will need to work in partnership with staff to resolve any issue

- Sanctions available include interview by a senior member of staff and, if appropriate, informing parents or carers.

- A pupil may have electronic communication access or computer access denied for a period.

- Denial of access could include all school work held on the system, including any examination work.

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

F Any complaint about staff misuse must be referred to the Headteacher.

Critical E-Safety incidents

A critical e safety incident is when unlawful or suspected unlawful material is found on any computer or digital device where criminal or inappropriate activity has or is taking place, or where an e-crime has been or is being committed. In such cases, the power lead should be taken out (not a normal shutdown) or the battery removed (laptop). Do not show (suspected) unlawful material to anyone else or undertake any further investigation; report to child protection officer in school and the ICT Unit immediately. Notes should be made that help in any subsequent local or police investigations.

Flintshire County Council takes all incidents of criminal activity very seriously and has worked with the North Wales Police Hi Tech Crime Unit to produce guidance on how to deal with critical e safety incidents. Appropriate action will be taken by Flintshire County Council and there may be occasions when the police must be contacted.

Extracts Dealing with Personal Use of Internet and Email

Use of Internet

Personal use of the Internet is permitted outside working hours and must be in a responsible and professional manner.

Sexually explicit material may not be intentionally displayed, archived, stored, distributed, edited or recorded using any Flintshire IT equipment.

Use of any Flintshire resources for illegal activity is grounds for immediate dismissal.

No employee or member may use Flintshire IT facilities to knowingly download or distribute pirated software or data.

No employee or member may use Flintshire Internet facilities to deliberately propagate any virus, worm, trojan horse, or trap-door program code.

Employees or members must not release confidential or sensitive information via a newsgroup or chat line, whether or not the release is inadvertent

No employee or member may use Flintshire's Internet facilities, including a web site or virtual learning environment, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

Use of Flintshire's Internet access facilities to commit infractions, which contravene any other policies and procedures in place within the Authority, such as the code of conduct and the harassment policy, are prohibited. Detail of such policies can be found under the relevant sections of the employee handbook.

Employees or members with Internet access may not use Flintshire Internet facilities to download images or videos unless there is an express business related use for the material.

Employees or members with Internet access may not use Flintshire Internet facilities to download entertainment software or games or to play games against opponents over the Internet.

It is not permitted to disable, defeat or circumvent any Flintshire IT security facility.

Use of Email

Incidental and limited personal use of email is permitted but must be in a responsible and professional manner and must not be misused or abused. The sending of any message which contains obscene material or offensive language is not permitted

Private use of email is allowed providing employee acceptance that monitoring of usage is in place.

Flintshire equipment may only be used for the Flintshire email system (Lotus Notes) and the School email system (Live@edu) and no other email systems may be used on Flintshire equipment.

Chain letters received must be forwarded to a designated mailbox.

Do not abuse others (known as flaming) even in response to abuse directed at you.

Dos and Don'ts of the new Live@edu / Office 365 email system.

- Do keep your username and password secure.
    - Do not share them with anybody.
    - Do log out when you have you have finished using the email service.

- Do manage your mailbox
    - Do use folders to organise your storage. It is possible to invite other colleagues and students to share folders and calendars in the cloud via email invitations.
    - Do delete e-mails from the cloud when no longer required - 10Gb might seem like a lot, but it will quickly disappear.

- Do not use the Live@Edu account for sensitive emails between the school and the Council e.g. child protection referrals. This mail should be sent from the Head's lotus mail account at the school.

- Do treat the 10 Gb Skydrive like an online secure [but not encrypted] memory stick.
  - ***Do keep a copy of essential files on school network*** – files placed in it are not automatically backed up.
  - Do anonymise all personal information in the Cloud wherever possible.
  - You <u>must</u> anonymise or password protect if you are saving sensitive documents to the skydrive, e.g. containing disciplinary or medical notes.
  - Do delete documents from the Cloud when no longer required