

## Clitheroe Royal Grammar School

### Information & Communication Technology Policy

Person(s) responsible: Assistant Headteacher (i/c New Technologies)  
ICT Network Manager

The primary function of ICT in schools is to facilitate learning. This could be in the classroom, at home, as well as the use of ICT for administration in school to enable procedures to be streamlined. It also encompasses the use of data to inform teaching and learning. This strategy also links closely to the aims of the school including:

- Develop lively, enquiring minds capable of original thought and well-balanced critical argument.
- Become confident, independent learners well-equipped for lifelong learning.
- Derive enjoyment from their learning which should extend their intellectual capacity, develop their interest and stimulate their curiosity.
- Embrace the many opportunities afforded by developments in information and communication technologies, whilst fully accepting the responsibilities that go with using them properly.

This policy reflects the school values and philosophy in relation to the safe teaching and learning of, and with, ICT.

This policy is intended for

- All teaching staff
- All support staff
- School governors
- Parents and guardians

#### Vision

21st century learners live in an ever changing world where the amount of information and knowledge is growing exponentially. Teachers can no longer be seen as the 'font of all knowledge' as students can access huge amounts of information/knowledge at the click of a button. The role of the teacher as facilitator is key; guiding students to explore, think and learn for themselves. The experience of the teacher is vital.

Learners need the skills to:

- **SEARCH** for relevant information and knowledge
- **ASSESS** the validity, reliability and bias of that information
- **EVALUATE** material
- **PROBLEM SOLVE** to find solutions logically
- **SYNTHESIZE** information
- **CREATE** and **DEVELOP** their own material
- **ADAPT** to and **EMBRACE** a constantly changing technological world.

#### Our aims for ICT

We aim for all students and staff in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which will enable them to use appropriate ICT resources effectively as powerful tools for teaching & learning. Our learners (students, teachers

and support staff) need to be comfortable with and skilful at navigating information and communication technologies.

To fulfil the above aims it is necessary for the school to ensure that:

- there is sufficient access to ICT, especially the internet
- ICT experiences are focused on enhancing learning
- skills (stated above) are embedded in the curriculum
- all users understand how to be safe (including personal safety, security of data etc.)
- there is a relevant ICT curriculum including ICT lessons and ICT used throughout the curriculum
- support and guidance from ICT specialists/technicians
- resources and equipment are kept up to date as much as possible
- all ICT is secure that is used in an appropriate manner
- cross curricular links are exploited where appropriate

### **Curriculum Development & Organisation**

All students have ICT lessons in Years 7, 8 and 9, where they learn to use software packages creatively and about how to be a safe and responsible ICT user.

Students also learn about online safety in ICT lessons. This is supported by further online safety and cyber-bullying sessions in Guidance as well as assemblies.

As well as the timetabled ICT lessons, a two-weekly online booking form is available for staff of all departments to sign up for additional time where appropriate (Main School). At York Street, the booking is done via the main office.

All staff are allocated their own personal laptops/netbooks as well as each teaching room being equipped with a PC, a digital projector and an interactive whiteboard (some departments opted to have a non-interactive whiteboard). In addition individual machines in staffrooms and departmental offices also support the development of ICT capability by enabling further development of tasks.

The ICT Co-ordinator is responsible for staff training and the development of ICT across the curriculum.

The Innovations group and more recently the Teaching and Learning Group are involved in exploring new and current methods of teaching and learning including the use of new technologies such as Web 2.0 technologies.

## ICT Management and Support

The school provides an appropriate level of support staff consisting of a network manager and two network technicians to maintain and support our resources.

It is important that hardware resources are maintained. It is intended, therefore, within budget constraints, to upgrade/replace equipment on a regular basis and annually sign up to Microsoft school agreement to ensure all operating systems and application software is also up to date. (See ICT Strategy for future plans and developments)

The school is committed to provide staff training on ICT to encourage and build confidence in the use of ICT. Training is regularly provided by the ICT Co-ordinator, keen teaching staff and the network support staff. Requests for training on any of the school's ICT resources are most welcome. Third party ICT training is also available for staff development.

Students are encouraged to make responsible use of ICT and the school has acknowledged the need to ensure that all students are responsible and safe users of the Internet and other communication technologies. A **Computer Usage and Internet Access Policy** has thus been drawn up to protect all parties.

## ICT Backup

The data on our two networks within the organization (Curriculum and Administration) is backed up in the following way: -

- A backup is taken every weekday evening.
- Monday to Thursday incremental backups are taken.
- On Friday full back ups are taken, rotated through a three week cycle.

At the end of each academic year a backup is made that is kept until the end of the next year. As well as this the user areas for Year 11 and Year 13 students are to be backed up to DVD and stored in a file for a five year period in case of plagiarism concerns.

## ICT Security

The objective of ICT security is to ensure school's continuity and minimise damage by preventing and minimising the impact of security incidents.

The purpose of the policy is to protect the school's information assets from all threats, whether internal or external, deliberate or accidental.

It is the school policy to ensure that:

- information will be protected against unauthorised access
- confidentiality of information will be assured
- integrity of information will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- ICT security training will be available to all staff

All breaches of ICT security, actual or suspected, will be reported to, and investigated by the ICT Network Manager.

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 daily.

### **Monitoring and evaluation**

It is the responsibility of each member of staff to adhere to the policy, standards and procedures.

The Assistant Head, working closely with the Network Manager and Head of ICT, has direct responsibility for maintaining the policy, standards and procedures and providing advice on their implementation.

Date of last review:	October 2011
Date of approval by Governors:	October 2011
Date of next review:	July 2012

## Appendix 1 Information , Communication and Technology statements

### Clitheroe Royal Grammar School

#### Information , Communication and Technology Statement (and Guidelines) for Teaching and Support Staff

##### Meanings

1. **school** means: Clitheroe Royal Grammar School (CRGS) as directed by its Governors, Headteacher and Senior Leadership Team (SLT)
2. **network/systems** means: any computer hardware or software owned, rented or leased by the school and made available to any teacher or support staff employed, whether directly or indirectly, by the school
3. **user** means: any person who uses the school's systems with the permission of the school either expressly or by presumption
4. **internet** means: the world wide web whether accessed online or offline by way of stored files, images or moving pictures howsoever stored and to include portable storage devices
5. 2 and 4 above can collectively be referred to as "**IT resources**"
6. **removable storage device** means: compact discs, DVDs, USB sticks, flash media or any other media that is capable of storing files, data, images, whether moving or still, or any other information that can be viewed or transferred from the device.

The use of the school's systems by the user is a benefit of the user's employment and one which the school actively encourages to enhance their contractual obligations for teaching and learning. Any deliberate breach of this policy will amount to a breach of the user's terms of employment and may result in sanctions being enforced under such contract of employment whether expressly or implicitly incorporated into the same.

The school retains and incorporates its absolute right, and will exercise the same at its absolute discretion, to monitor, by whatever means it deems suitable, all systems and internet access records stored on, or processed through, any school network or system or the CRGS and/or Lancashire Education Authority (LEA) servers.

Accordingly the school has determined the following rules and guidelines for the use of its IT resources which may be amended as and when the school deems fit to do so.

##### Rules

It is forbidden for a member of staff to:

1. deliberately disclose any information to an unauthorised person or organisation which is contained on the school's network. An unauthorised person or organisation is any entity not directly connected to the school's Senior Leadership Team or any entity who the user does not truly believe is entitled to receive such information
2. access any user accounts other than by their own authorised accounts and password or deliberately disclose the same to another person, save, that person having express permission, or implied permission by the nature of their employment description, from the Headteacher / SLT to do so
3. access any files, data or other resources of other users which may be stored on the network unless such files, data or resources are open for common view in public / shared areas
4. deliberately engage in any activity that affects, or threatens to affect, the integrity of the network or any files, programs or systems contained thereon

5. deliberately send an e-mail or post online (e.g. on Facebook) any message that contains, or has an attachment which contains, defamatory, insulting, offensive, racist, violent or threats of violence, indecent and/or obscene words or images, chain letters or any other item that the user should reasonably know is an unacceptable subject, image or content within a school environment or that is likely to bring the name of the school into disrepute
6. view any indecent / obscene, racist or violent material on the school's resources, to include laptop computers whether on school premises or not
7. use the school's IT resources for personal financial gain, gambling, promotion of personal political views or advertising anything that the user has not had prior written permission from the Headteacher or Governors to advertise
8. use the school's IT resources to access any chat room or forum not hosted by an educational site recognised by SLT and / or LEA
9. use the school's IT resources to post anonymous messages on any system or network
10. download any third party unlicensed program or file from the internet or removable storage device without written permission from the Headteacher / Network Manager / Computer Technician
11. copy programs or data which the user does not have authority to do so. The copyright of all materials used should be respected.
12. publish, or cause to be published, whether directly or indirectly, on the internet or via e-mail any material or data which identifies, whether directly or by implication, Clitheroe Royal Grammar School, its staff, governors or pupils, whether past or present, without the full written permission of those persons identified and the Headteacher.

Members of staff should:

1. ensure that personal social networking sites are set at private and students are never listed as approved contacts
2. not give their personal contact details to students, including their mobile telephone number
3. only use equipment e.g. mobile phones, provided by school/service to communicate with students, making sure that parents have given permission for this form of communication to be used
4. only make contact with students for professional reasons
5. recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible
6. not use internet or web-based communication channels to send personal messages to a child/young person

### **General guidelines**

The school offers the following guidance as to the user's use of the school's IT resources to protect both the user and the school:

1. Always keep account names and passwords confidential and change passwords regularly
2. Passwords should be a strong password; combination of letters, numbers and special characters and should use both lowercase and capital letters.
3. Always store your files and data in your own secure area on the network or, preferably, on a removable storage device.
4. Users should not log on to or use any account other than their own and should log off or lock workstations when leaving them, even for just a short period of time. This includes computers at home if sensitive/confidential school data is being accessed.
5. Back up your files and data regularly, preferably in duplicate, including whilst in use
6. Never access any file, e-mail attachment or program if you are not absolutely sure of its nature or origin or which you do not have the authority to access. If in doubt, do not open it and report the file or program to the Headteacher / Network Manager / Computer Technician.

7. Do not store sensitive/confidential data about pupils on portable devices such as pen drives, unless the data is encrypted or password protected.
8. Members of staff should also be circumspect in their communications with students so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. This would include using formal language and layout in emails.

### **Social networking sites guidelines**

Employees who choose to make use of social networking site/media are advised as follows:-

- Familiarise yourself with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;
- Do not conduct or portray yourself in a manner which may:-
  - bring the school into disrepute;
  - lead to valid parental complaints;
  - be deemed as derogatory towards the school and/or it's employees;
  - be deemed as derogatory towards pupils and/or parents and carers;
  - bring into question their appropriateness to work with children and young people.
- Do not form on-line 'friendships' or enter into communication with \*parents/carers and students as this could lead to professional relationships being compromised.
- On-line friendships and communication with former students is strongly discouraged particularly if the students are under the age of 18 years.

(\*In some cases employees in schools are related to parents/carers and/or students or may have formed on-line friendships with them prior to them becoming parents/carers and/or students of the school. In these cases you are advised that the nature of such relationships has changed and that you need to be aware of the risks of continuing with this method of contact. You are advised that such contact is contradictory to the guidelines above).

### **E-mails**

The school recognises that the use of e-mail is a valuable, widely used, quick and cost effective method of communication. It can also be a prolific host for computer viruses, chain letters, pornography and many other items that are unacceptable in the school environment. Users are strongly advised to be extremely careful when utilizing this form of communication.

As such the user is forbidden to:

1. use their official e-mail address other than for purposes of representing the school in an official capacity
2. open or view any e-mail not personally addressed to them using their own authorised e-mail address.

It is highly recommended that the user only uses his/her official e-mail address at all times when communicating with other members of staff, school governors, school trustees, other schools or their staff members and governing bodies, businesses and organisations providing goods or services to the school, internet sites as a direct consequence of the user's research for authorised school activities or other sites whilst representing the school in an official capacity. Use of a personal e-mail address in the preceding circumstances should only be done if absolutely necessary and in circumstances where the user considers it absolutely necessary to perform their duty as an employee.

The school does not encourage, but will allow, the user to send and receive personal e-mails, sent to their non official e-mail address(es), via the school's IT resources. However, it is the user's full responsibility to ensure that, when sending or receiving personal e-mails via the school's IT resources, no breach of the rules defined herein is committed. It is highly recommended that the user adheres to the same rules for e-mails sent on their personal accounts as on their school accounts.

It is strongly advised that formal language and layout is adhered to whilst using school email accounts, as members of staff are representing the school in their professional capacity.

### **Use of YouTube**

YouTube can be accessed by members of staff in school. This should only be accessed for educational purposes within school. Staff should ensure that the content is appropriate for use in school before it is shown to students.

### **Procedure for photographs of students / staff**

If you take photographs of students and / or staff for school events or trips etc, please follow the following procedure:

- after editing photos on your school laptop or home computer, transfer them onto a USB stick
- bring the USB stick into school and have them transferred onto the CRGS media drive located in the Chatburn Road IT office
- please then delete the photographs from your school laptop / home computer and the USB stick
- for any photos that are used for publications such as the Yearbook, the school website etc, students featured should be checked to see if permission has been given for use of their image. Jasmine Renold and Amanda Payne have the appropriate list.

### **Responsibilities**

- It is a user's responsibility to look after the equipment that they are using.
- Users should report any broken or malfunctioning equipment to an ICT technician as soon as possible.
- Users are required to respect the privacy of others and the reputation of the school.
- Users should remain vigilant for any breaches of school ICT security and contact the appropriate staff if issues are uncovered.
- It is the user's responsibility to ensure that it does not cause offence or anxiety to others, or infringe copyright.
- ICT systems are there for the benefit of the entire institution; activities that waste technical support time and resources are prohibited.
- **All users must sign and return this "Information , Communication and Technology Statement" before using any school's ICT equipment.**

### **Protocol for investigating matters relating to inappropriate computer use**

Students and staff are aware that all computer network use is monitored within school. If there is suspicion of inappropriate use or if it becomes apparent that mis-use of the school network has occurred then this will be investigated by the ICT Network Manager and his staff. Any suspected misuse by staff must be referred to the Headteacher before an investigation takes place. The Headteacher (or, in her absence, a Deputy Headteacher) will always be notified if inappropriate material is suspected or discovered.

**Protocol for investigating matters relating to students, staff or the school community which may necessitate accessing the internet**

On occasion, it may be necessary to conduct an investigation into internet activity which has been brought to our attention.

Most of these investigations will be dealt with by the Senior Leadership Team and the ICT Network Manager, although other staff may be involved with their consent. Any investigation that may require use of the internet must be discussed with the Headteacher (or, in her absence, a Deputy Headteacher) before the investigation occurs.

The Senior Leadership Team and ICT Network Manager would not be required to investigate a matter relating to anything of a sexual nature / inappropriate images as this would need to be discussed with the Lancashire County Council Safeguarding Team and passed on to the appropriate body.

Social networking sites cannot be accessed via the school network. Therefore, on occasion, the Headteacher (or, in her absence, a Deputy Headteacher) may request that a member of the Senior Leadership Team or ICT Network Manager use their home internet access to investigate the matter. The Senior Leadership Team and the ICT Network Manager must not investigate any matter without the full knowledge of the Headteacher and / or another senior colleague.

Following an investigation, printouts may be kept on file if the Headteacher felt it appropriate.

All investigations into inappropriate activity should be logged in a central location.

***Further advice and guidance can be found in the “Guidance for Safer Working Practice for Adults who Work with Children and Young People”. (March 2009)***

**CLITHEROE ROYAL GRAMMAR SCHOOL**

**Acceptable Network & Internet Use Statement  
For Students Years 7 to 11**

The computer systems are owned by Clitheroe Royal Grammar School and are made available to students to further their education. The school's ICT Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer systems. The content of all internet sites visited by students will be monitored by the IT staff.

All students should return a signed acknowledgement slip to school.

The school reserves the right to withdraw access to IT resources from any student who behaves in an inappropriate manner.

Internet access is filtered by the Local Education Authority. However, no filtering system is perfect. If your son/daughter accesses any material that they find disturbing (deliberately or accidentally), they should report it immediately so that it can be blocked.

- All internet activity should be appropriate to the student's education;
- Network access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of all materials must be respected;
- Posting anonymous messages, forwarding chain letters or using chat programs is forbidden;
- As e-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden;
- Downloading or installing any third party programs is forbidden;
- Students are forbidden to take photographs or video of staff or students without prior permission;
- Material (text, video, photo) about the school and/or persons connected with the school are not to be published on the internet (e.g. Facebook) without prior permission from the Headteacher;
- Any activity which in the opinion of the school is inappropriate or brings the name of the school into disrepute is forbidden, including use of internet sites at home.
- Students should report any incidence of cyber-bullying to your Head of Year and /or the Network Manager.

Depending on the severity, any student disobeying this policy will experience sanctions including suspension up to permanent exclusion.

-----

To be completed by the Parent/Guardian:

I have made my son/daughter aware of the need to adhere to the Acceptable Network & Internet Use Statement and he/she understands that visits to Internet sites may be monitored by IT staff.

Pupil's Full Name ..... Form .....

Parent's Signature ..... Date .....

**CLITHEROE ROYAL GRAMMAR SCHOOL**

**Acceptable Network & Internet Use Statement**

**For Sixth Form Students**

The computer systems are owned by Clitheroe Royal Grammar School and are made available to students to further their education. The school's ICT Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer systems. The content of all internet sites visited by students will be monitored by the IT staff.

Students requesting network/internet access should sign a copy of this Acceptable Network & Internet Use Statement and return it to the IT Office (in room 6) for approval. The school reserves the right to withdraw access to IT resources from any student who behaves in an inappropriate manner.

Internet access is filtered by the Local Education Authority. However, no filtering system is perfect. If your son/daughter accesses any material that they find disturbing (deliberately or accidentally), they should report it immediately so that it can be blocked.

- All internet activity should be appropriate to the student's education;
- Network access should only be made via the authorised account and password, which should not be made available to any other person;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Copyright of all materials must be respected;
- Posting anonymous messages, forwarding chain letters or using chat programs is forbidden;
- As e-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden;
- Downloading or installing any third party programs is forbidden;
- Students are forbidden to take photographs or video of staff or students without prior permission;
- Material (text, video, photo) about the school and/or persons connected with the school are not to be published on the internet (e.g. Facebook) without prior permission from the Headteacher;
- Any activity which in the opinion of the school is inappropriate or brings the name of the school into disrepute is forbidden, including use of internet sites at home.
- Students should report any incidence of cyber-bullying to your Head of Sixth Form and /or the Network Manager.

Depending on the severity, any student disobeying this policy will experience sanctions including suspension up to permanent exclusion.

-----  
To be completed by the student:

I agree to adhere to the Acceptable Network & Internet Use Statement and understand that visits to Internet sites may be monitored by IT staff.

Full Name: .....

Form: .....

Signature: .....

Date: .....