(Updated June 2016)

This policy document sets out the school's aims, principles and strategies for the delivery of Computing and the use of IT. This policy was developed in the summer term 2007 and is revised on an annual basis. Reference is made to the other school policies e.g. Health and Safety.

1. Definitions used in this policy

We interpret the term *'IT'* to include the use of any equipment which allows users to communicate or manipulate information (in the broadest sense of the word) electronically.

We interpret the term *'Computing'* to be the curriculum subject concerned with how computers and computer systems work, how they are designed and programmed, how to apply computational thinking and how to best make use of information technology (IT). The three main strands within Computing are Computer Science, Digital Literacy and Information Technology.

'ICT' is a subject studied at GCSE and A Level by some students.

2. The significance of Computing

A high-quality computing education equips pupils to use computational thinking and creativity to understand and change the world. Computing has deep links with mathematics, science and design and technology, and provides insights into both natural and artificial systems. The core of computing is computer science, in which pupils are taught the principles of information and computation, how digital systems work and how to put this knowledge to use through programming. Building on this knowledge and understanding, pupils are equipped to use information technology to create programs, systems and a range of content. Computing also ensures that pupils become digitally literate – able to use, and express themselves and develop their ideas through, information and communication technology – at a level suitable for the future workplace and as active participants in a digital world.

(National Curriculum for England, Department for Education 2013)

3. The school's aims for IT/Computing

The school aims to ensure that teachers develop the confidence and competence to use IT as an effective aid for teaching and learning in their subject. All learners should have access to a modern, effective IT infrastructure. We also aim to use IT to facilitate effective administration and communication.

The overall aim for Computing is to enrich learning for all pupils. Computing offers opportunities for pupils to:

- understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation
- analyse problems in computational terms, and have practical experience of writing computer programs in order to solve such problems

- evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- become responsible, competent, confident and creative users of information and communication technology
- enhance their learning experience in all subjects.

4. The school's curriculum organization

4.1 Key Stage 3

All students in Years 7 and 8 have one discrete Computing lesson a week consisting of a mixture of Digital Literacy, IT and Computer Science lessons.

4.2 Key Stage 4

In Year 9, students develop their knowledge of Computing in their lessons of other subjects, reinforcing what they have learnt in the first two years.

Key Stage 4 students can choose to study GCSE Computer Science, with some students also developing their capability, creativity and knowledge in digital media and IT by taking GCSEs in ICT, Music, Art or Media Studies.

Entry Level Courses and CLAIT are offered to students where these are considered to better meet the needs of pupils.

A cross-curricular provision for Computing for all students is currently being developed in the core subjects.

4.3 Key Stage 5

A Level Computer Science and A Level ICT are offered as options.

5. Responsibilities

5.1 SMT / Leadership team

There may be instances when there is an overlap between this policy and other school policies. In these cases members of the Senior Management Team and the Leadership should ensure that their policies are carried out in full.

5.2 Computing Coordinator

The Computing Coordinator/Head of Computing is responsible for the delivery and development of Computing in the school.

- Coordination
◊ writing Computing Department Development Plan
◊ development, writing and implementing of the whole school IT/Computing policy
◊ coordinating delivery of Computing across the curriculum
◊ advising in the production of departmental Computing policies
◊ ensuring that the school IT/Computing policy is being implemented
◊ ensure the delivery of NC Computing

- Monitoring and reviewing
◊ Enforce, quality audit and review the IT/Computing policy

- Resources

◊ keeping up to date in developments in Computing

- Staff development and support

◊ Liaising with staff to identify Computing INSET needs

- Liaison

◊ Liaising with the Advisory service
◊ Keeping up to date with developments in the application of Computing in the curriculum
◊ With the e-Safety Coordinator on monitoring and developing the provision for e-safety
◊ With staff/departments on use/development of Computing

◊ Head of Computing (See Computing Department Handbook)

5.3 e-Safety Coordinator

- Prepare and assist with the delivery of assemblies on e-safety
- Develop and Review the delivery of e-safety issues within discrete and cross-curricular Computing lessons
- Raise the level of awareness of e-safety issues for staff, students, parents and other members of the school community
- Stay up to date with e-safety developments, in particular with regard to emerging technologies
- Assist Computing Coordinator with the development and implementation of e-safety policies
- Ensure staff are trained on e-safety issues
- Ensure that e-safety policies are enforced and are up-to-date
- Responsible for checking that Acceptable Use Policies and e-safety material are being displayed on school notice boards and are publicised on school web site
- Review the e-safety policy and provision on an annual basis

5.4 Network Manager

The Network Manager is responsible for the IT infrastructure.

- Resources

◊ coordination of the purchase of IT resources
◊ responsible for the maintenance of equipment through IT technician liaison
◊ liaising with departments on IT resource needs
◊ coordination and management of the provision of resources (booking system, consumables)
◊ keeping up to date in developments in IT
◊ monitoring all IT labs
◊ responsible for school website

- Staff development and support

◊ Liaising with staff to identify IT INSET needs

- Liaison

◊ Liaising with the Advisory service

5.5 All Staff

All staff should be aware of this IT/Computing policy and ensure that they, and the students that they teach, follow it. In addition staff should:

- Make appropriate use of IT, including the VLE, in enhancing learning and teaching
- Ensure that all pupils within their teaching groups have access to IT facilities
- Ensure any faults discovered in lesson time are reported to IT department for repair
- Follow all security procedures for IT equipment issued to them, particularly laptops
- Bring in portable equipment for testing (e.g. laptops), on request
- Report any accidental breaches of the Acceptable Use Policy
- Report any inappropriate / illegal misuse of school IT facilities
- Report any web sites that students should not have access to that are currently not being prevented by the filtering system
- Ensure IT rooms are locked, windows closed and room plans have been completed and submitted, at the end of every lesson
- Be aware of e-safety issues and ensure that this is reflected in their teaching practice
- Continue to develop their own Computing competence and their teaching practice with the use of IT
- Aid their departments in the development of good IT/Computing practice
- Turn off any air-conditioning units at the end of each lesson
- Ensure that all IT requests (e.g. room bookings) are submitted no later than the Tuesday preceding the week they are required.
- Complete an annual audit of any IT equipment issued to them
- Structure and plan IT use to include all students in a class
- Avoid personal use of the IT facilities during lesson times
- Ensure that they do not infringe copyright and licensing laws

6. Access to IT Resourcing

The school has six networked computer rooms that are timetabled for classes throughout the week. The school also has dedicated Photography, Media and Music IT suites and various sets of wireless laptops.

All classrooms are connected to the school network. Additionally there are banks of laptops which link to the computer network by wireless technology and sets of desktop computers in various departments, as well as sets of desktop computers in some departments. All classrooms are connected to the school network.

Interactive Whiteboards are installed in most rooms, together with digital projectors where appropriate.

All discrete ICT/Computing/Computer Science lessons take place in computer rooms. Lessons in other subjects can also request to use IT rooms, generally on a first-come first-served basis.

IT facilities are available after-school and before school, but as with lesson bookings this needs to be checked with the Network Manager first. In general, computer access for students is available in the library from 8:30am to 5:00pm. Room 34 is open at lunchtime for student use; priority is given to students who need to do school work.

All departments have access to data projectors. All teaching staff are issued with a laptop, with core software installed, though the laptop remains the property of the school. IT resources are normally purchased by the Network Manager; however, departments can also complete their own purchasing. In the latter case, advice can

be obtained from the technical support team and departments must inform the technical support team about the purchases for security reasons. Departments are to speak to the technical support team prior to purchasing to avoid any potential problems.

The Network Manager maintains an audit of IT equipment that is updated on an annual basis. It is the responsibility of staff to complete the audit for any equipment with which they have been issued.

7. Inclusion

All pupils, regardless of race, gender, disability shall have the opportunity to develop Computing capability. The school will promote equal opportunities for computer usage and fairness of distribution of IT resources. Children with a computer at home are encouraged to use it for educational benefit and parents are offered advice about what is appropriate. Any parents who have financial difficulty in the purchase of IT equipment should contact the Headmaster, in writing.

Work created at home can be transferred to a classroom computer by either e-mail, using the VLE or portable storage devices.

When pupils are completing paired work, 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 more able IT users always with less able pupils. 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 advantages of the use of IT by children with special educational needs.

Using IT can:

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

Staff should structure their IT-based teaching materials to match specific learning difficulties, in the same way as they do their other materials. If the situation arises, the school will endeavour to purchase appropriate resources to suit the specific needs of the child.

8. Technical Support

The Network Manager will line manage the technical support team. The team consists of the Network Manager, a Senior IT Technician and three IT Technicians.

In addition, the school make use of external companies to provide additional support as needed.

9. Monitoring and review

There is an annual review of this policy by the Computing Coordinator and other stakeholders.

10. Acceptable Use Policy

The school has an Acceptable Use Policy that all users of computers on the school network have to read and accept before they can log on. If they do not agree with the Acceptable Use Policy then their log-in will fail.

Staff issued with school laptops agree to follow the Acceptable Use Policy on these laptops (though the AUP will not be displayed on these machines when they log in). Staff also are to ensure that laptops are stored securely and sign a declaration on how laptops are used (for tax purposes).

The AUP applies to all staff and students using IT equipment, when in school and when using school equipment outside school.

See 16.4

11. Health and Safety/Security

Portable equipment and computers will be checked annually under the Electricity at Work Regulation 1989. It is the responsibility of all staff to ensure that any portable equipment they are issued with (e.g. laptops) is made available on request so that electrical safety can be tested.

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. ICT Room Rules (see section 11.1) are also on display in the relevant rooms for reference along with specific rules for the use of Internet and E-mail.

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 pupils which meet these requirements. More details can be found in the School Health and Safety Policy.

Computer rooms are locked overnight and have additional security measures in place. The school has an alarm system installed throughout. The files and network system are backed up regularly. The virus checker is updated regularly automatically.

Rooms 34 and 65 have air conditioning units that should be used when lessons are taking place. Please do not open the windows as this negates the affect of the air conditioning. It is the responsibility of class teachers to turn the air conditioning off at the end of a lesson.

It is vitally important that all windows in IT rooms are closed at the end of every lesson to prevent rain damage.

11.1 IT Room Rules

Food and drink is not to be consumed near computers

Ensure that all bags are underneath desks

Doors and windows should be closed at the end of each lesson

Any faults with equipment should be reported to your teacher or to the IT Department

Do not try to fix equipment yourself

During lessons, you should only use the programs / web sites that your teacher has asked you to use

Outside of lessons you may use the computers for games, general surfing etc…, but priority will be given to those needing to complete work

All behaviour in IT rooms must be sensible – including no running and not messing around on any wheeled chairs

You must read the Acceptable Use Policy, and follow the rules it states in order to use the computers

12. Copyright and licensing

Only the Network Manager can authorise the installation of software on the school network. Personal software must not be loaded onto school computers. Software can only be installed in-line with license agreements.

13. Career Professional Development and Training

There is a regular audit of training needs, which will be used when planning the CPD programme. Training on e-safety using interactive whiteboards and SIMS form a regular part of the CPD programme. Training is open to all teaching and ancillary staff. Training on using FirstClass is provided by the Technical Support Team; advice on using the VLE is provided by the Computing Department.

14. Use of Pupil Images and Pupil Personal Details on School Website

If an image of a pupil is on the school website then there must be no reference to their name. If a pupil is named on the school website then their photo must not be shown. No further personal details about the student should be on the school website. New materials added to the school website will be checked for compliance with this by the Network Manager. If any member of staff sets up their own website then they must follow this policy in full.

15. Use of Internet Policy

All pupils and staff have access to the Internet, both during lessons and at other times. All Internet usage should be legal and appropriate, as laid out in this policy document and in the acceptable use policy.

Any violations (even if accidental) should be reported to the Network Manager.

Staff should take care when using Internet sites, especially during a lesson. Websites should be vetted for appropriateness before being shown (or recommended) to pupils. Staff should also check (well in advance) that the school filtering system does not affect websites or online services they wish to use – any problems should be referred to the Network Manager.

It is recommended that staff do not use search engines in lessons as there is no guarantee of what the search results will return – this is particularly true when doing image searches. Staff are recommended to bookmark sites/resources they intend to use prior to the lesson.

The school will accept no responsibility for loss caused by credit card fraud (or similar) from the use of the Internet, and it is recommended that any important personal business is not done on the school's network. Staff should not use the Internet for personal use during lesson times.

If staff, or pupils, are creating their own websites, podcasts, wikis, blogs, or are using social networking sites (e.g. Facebook, Twitter) then due care must be taken and usage must be appropriate. This applies whether this is being done in or out of school. Pupils must not give out personal information to people they do not know, and they must not arrange to meet anyone they have contacted over the Internet without first obtaining the permission of their parent or teacher. Staff must never allow a pupil to be their friend on a social networking site. Only FirstClass should be used when emailing students (unless otherwise agreed by SMT) and teachers should never use their own mobile phones to contact students.

Pupils are allowed to use the Internet outside of lessons, but are only allowed to access the Internet during lessons if the class teacher has given permission.

15.1 Teaching and Learning - Use of Internet

All staff have a responsibility for encouraging students to use information found on the Internet appropriately. Staff should ensure that they take every opportunity to:

- Discuss copyright issues e.g. just because something can be found on the Internet does not mean that you are allowed to copy/use it.
- Encourage the use of material that is copyright free / released on a Creative Commons License (or similar).
- Discourage students from copying and pasting material – work which is just copied and pasted should be redone. Using a search engine it is normally easy to check if work has been copied and pasted from a web page.
- Encourage students to acknowledge their sources of information.
- Discuss the reliability of information – anyone can create a webpage so just because information can be found on a website does not mean that it is correct. Methods for checking the reliability of information include using multiple sources and considering the provenance of a source.
- Consider issues relating to biased information

16. e-Safety

At Trinity, we place a great deal of importance on ensuring that our students are able to work in a safe and secure environment and take all appropriate steps to achieve this aim.

16.1 E-mail

Email can be an extremely valuable tool in an educational context, encouraging the development of communication skills, and transforming the learning process by opening up possibilities that, conventionally, would be impossible to achieve. However, there are a number of issues for consideration when using email in the school such as the management implications of implementing email, and acceptable use of email by pupils. Other issues, such as bullying by email, are emerging which schools also need to be concerned with.
(BECTA)

Staff and students have an email address within FirstClass. A safe-house email system is used – students are only able to send/receive emails to/from other holders of a Trinity email account. This prevents students from receiving inappropriate mail

from outside the school. The safe-house facility can be temporarily disabled if teachers want students to contact people outside the school for an educational purpose. Teacher email accounts are not in the safe-house allowing them to contact external bodies as required. Some staff have email accounts provided by Redbridge in addition to their FirstClass account.

While the filtering and safe-house reduce the likelihood of email misuse, they do not prevent students from sending abusive or bullying emails to each other. If access to email is allowed then this problem is impossible to prevent, however we closely monitor what pupils send by email, using the Securus software. Sending abusive or bullying emails is not accepted in Trinity and will be dealt with most severely.

Students must only e-mail people that they know. All staff and student use of e-mail must be appropriate; all messages must be polite and responsible.

16.2 Filtering

While the Internet is an excellent source of material for use in lessons, there is a large amount of inappropriate material available to which pupil access needs to be prevented. The school has a filtering service in place to help prevent access to these sites, a walled garden being too limiting for students at a secondary school.

The filtering service is run by the Internet Service Provider, providing a higher level of security and less chance of individuals tampering with settings. The filtering works on a category basis, where websites are categorised according to type and the school selects which categories we wish to filter. In addition to this, there is a local deny list to which we add specific sites that we want to filter; and just as importantly a local allow list which we use to allow access to specific sites that are in categories that we want to be filtered.

No filtering service is 100% effective and the local deny list and categories are updated on a regular basis. The Securus software and teacher comments are used to help monitor the effectiveness of our filtering service. Teachers are encouraged to test all websites that they wish to use in lessons on the school's machines to ensure that the filter allows access to these sites.

Staff must inform the Network Manager if they come across any inappropriate sites whilst using machines on the school network that should be added to our local deny list.

Attempts to deliberately circumvent the filtering system will be treated as a serious offence.

16.3 Viruses

Viruses and other malware can severely disrupt the service on a network, as well as causing loss of data. The school have a subscription to corporate anti-virus software to help detect and remove viruses. The software updates automatically to ensure that protection is effective.

All staff and students must take appropriate measures to help prevent the school network becoming infected by malware. It is important that all network users ensure that they have appropriate malware prevention (e.g. anti-virus software) at home to help prevent the spread of viruses. Staff and students should take care about opening e-mail from unknown sources (especially e-mails with attachments) and they should not download programs from websites of unknown reliability.

16.4 Copy of Acceptable Use Policy

RULES FOR RESPONSIBLE PC USE

The school has installed computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- I agree that, although the school has a robust backup system in place, I will also keep a backup of all my important files and documents;
- I agree that, if I have a problem, I will tell my teacher or the IT Technicians immediately;
- I will only access the system with my own login and password, which I will keep secret;
- I will not access other people's files;
- I will only use the computers for classwork and homestudy, except when given express permission otherwise;
- I will use virus checking software to check any data I bring on CDs or other media from outside school, prior to using it on the school's computers;
- I will ask permission from a member of staff before using the Internet in lessons;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address, telephone number or other personal details, or arrange to meet someone unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me;
- I understand my report would be confidential and would help protect other pupils and myself;
- I understand that the school check my computer files and monitor the PC for inappropriate use and improper Internet sites I visit;
- I understand that the school filter my access to the Internet;
- I will not try to deliberately circumvent the school filter;
- I understand that any inappropriate use may result in disciplinary action;
- I will not attempt to cause any damage to the computer system, including the introduction of viruses or deliberate deletion of files, as well as physical damage;
- I will not install any software without receiving permission from the Network Manager or IT Technicians first;
- I will not keep movie or music files on the school system, apart from those needed for schoolwork;
- I will report any accidental breaking of any of these rules to the IT Department;
- When doing any work I will acknowledge all the websites from which I have obtained information;
- I will not copy other people's work, or material from a website, and claim it is my own;
- I will not post any material about myself, or people at the school, on a blog/social networking site/etc... (e.g. Twitter, Facebook) that could be deemed offensive or could lead to endangering myself or others;
- I agree that personal use of the school network will only take place outside of working hours and that the school accept no responsibility for any problems that may arise from such personal use;
- I agree that priority for computer usage is given to those who need to complete school-related work;

- I understand that if I am using the school's computers that I have agreed to follow these rules;
- I understand that all use of the school computers should be legal, appropriate and moral; these rules do not cover all possible infringements and I will comply with the intention behind these rules as well.

16.5 Securus terminal monitoring software

This highly-effective software looks at everything that is displayed on any terminal on the school network – including images, content of web sites, contents of all email messages and everything that the user types into any piece of software – and stores a screen capture of any violations. The IT Technicians regularly look at all reported violations and all positive violations are reported to the relevant member of the pastoral team. Inappropriate language / material are not accepted at Trinity and infringements will be dealt with severely.

This software detects inappropriate language, pornographic material, racism and bullying. The extensive dictionary can also be added to locally allowing us to check for use of any specific word.

Students and staff are made aware that their activity on the school computers is monitored.

16.6 e-Safety Education (Students)

e-safety is taught as part of the Key Stage 3 and 4 Computing Schemes of Work; though all staff are expected to be aware of the issues that can arise and advise students appropriately during lessons where IT equipment is being used.

Year 7
On arriving at Trinity, Year 7 students are made aware of how to use FirstClass (the school's Virtual Learning Environment) appropriately and the acceptable use policy that they must adhere to. Sanctions for breeching acceptable use are made clear to students. They are made aware that all the communication they make on FirstClass can be monitored and unsuitable websites are flagged up and checked.

There are 2 units of work centered on e-safety. One is looking at the dangers of cyberbullying and the ways in which to prevent it. Students also look at the reliability of information they find online and learn that they cannot trust everything they read.

Year 8
At the start of Year 8, students are reminded of the acceptable use policy. They examine possible scenarios which breech the acceptable use policy of the school and discuss how they could be avoided.

Students complete a unit of work where they create a fake website. They are asked to consider what the dangers of fake websites are (e.g. giving false information, taking your details for unscrupulous means). Students look at examples of fake websites and consider how they can spot one for themselves.

Students also complete a unit of work where they plan and make their own 'fake' airbrushed images. Here students consider the impact of airbrushing on self-esteem. In addition, they discuss how bullies could use image manipulation as a means to torment their victims.

Key Stage 4

Students in Year 11 have the opportunity to work toward a GCSE in ICT.

E-safety is referenced explicitly in the unit Staying Safe Online where students focus on the inappropriate sharing of personal data, using inappropriate language and discuss appropriate steps to avoid inappropriate disclosure of personal information. They learn about the use of codes of conduct for personal protection.

Implicitly e-safety is referenced throughout the course and security issues relating to e-safety are built into many areas of this GCSE. For example, when studying information handling students look at the importance of passwords and while learning about email students consider how email can be misused and how such misuse can be avoided. Health and safety issues are also explored.

All Students
There is a programme of whole year assemblies given by Year Heads on e-safety issues. In the last few years, ChildNet International and Copperex have also visited the school to deliver e-safety days.

There are also e-safety themed activities completed during circle time and reading periods throughout the year.

16.6 e-Safety Education (Parents)
The school strongly believes in supporting parents in ensuring that students stay safe online when at home as well as in school. The school website has a regularly-updated section on e-safety and this is used as a portal for disseminating advice and information on e-safety issues.

16.7 e-Safety Education (Staff)
Staff are expected to be aware of e-safety issues – what they are, how to recognise dangers and what to do if an issue arises. All new staff receive inset on e-safety. Also there are e-safety inset sessions that all staff are welcome to attend and annual CPD for all staff on child protection (including e-safety) issues.

17. Mobile Phone/Camera Phone Policy
See Pupil Journals

18. Staff Code of Conduct
Trinity staff agree to use IT facilities in an appropriate manner and follow the IT Code of Conduct (copy on the next page).

Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's IT policy for further information and clarification.

- I understand that to use the school IT system for a purpose not permitted by its owner is a disciplinary, and potentially criminal, offence.
- I understand that IT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that school information systems may not be used for private purposes during working hours without specific permission from the headmaster.
- I will not use the IT facilities for commercial or financial gain.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. This includes personal data stored on laptops, memory sticks and all other IT equipment.
- I will respect copyright and intellectual property rights. If I am unsure I will not use the material.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headmaster.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I will not communicate with students on social networking sites or allow students to be a "friend" on these sites.
- I will ensure that any communications with students via e-mail (or any other electronic communication system) will be over the school provided e-mail system only – unless written permission has been obtained from a member of the senior management team.
- I will never use school equipment or facilities, or allow them to be used, to view or download any material likely to be unsuitable for children. This applies to any content of a dangerous, violent, racist or inappropriate sexual nature, etc…
- I will ensure that usage and content of any personal websites, blogs or similar is appropriate.

- I will ensure that any material placed on social networking sites (or similar) will not constitute an e-safety issue or could be interpreted as being derogatory to a student or member of staff at Trinity.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and the content they access or create.
- I will report any infringements (even if accidental) of the code of conduct.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for IT.

Signed: …… Print: …… Date: ……

Accepted for school: …… Print: ……

18. Use of School Laptops Agreement
Attached to this policy are copies of sheets issued to all staff:

- Advice on security of staff laptops
- Declaration on use of laptops (for tax purposes)

If a laptop is lost or damaged then this needs to be reported to the relevant Director of Site and the IT Department.

If there are any problems with IT equipment or IT equipment is damaged then this should be reported to the Network Manager.

Security of School Laptops

1. The equipment is issued to the named member of staff and remains that persons' responsibility

2. The equipment is covered under school insurance, provided that the following precautions are taken.

    - **On School Premises**
        - Equipment should not be left in classrooms or unlocked offices
        - Equipment must be locked away when not in use
        - Equipment must not be stored in classrooms overnight
        - If equipment is loaned to other members of the department they must be made fully aware of all precautions to be taken
    - **Outside school premises**
        - Equipment must be stored securely, not left on display
        - Equipment must not be left unattended in cars

Please regard this as a written instruction on behalf of the Headmaster.

TRINITYCATHOLICHIGH SCHOOL

(Science and Sports College)

Headmaster: Dr. P.C. Doherty, B.A., D.Phil (Oxon),.F.R.S.A.
Website: http://fc.tchs.uk.net

Statement on personal usage of IT Equipment

Name: _____

Make of Laptop: _____

Please tick the statement that applies to your use of this equipment:

[ ] The laptop is never taken off school premises

[ ] The laptop is taken off school premises but there is no personal use of this equipment

[ ] There is personal use of this laptop

Signed:

_____

Date:

_____