St Ursula's Convent School ICT Policy

1) The aim of the school

a) To create a community in which all pupils can grow as Christians and achieve their potential academically and socially, which will enable them to take their place in society.

2) A Christian Community

a) The faith of the Catholic Church and the values of the gospel message underlie all that the school seeks to accomplish.
b) Faith is expressed and fostered in collective worship, in the work and activities of the RE department and in all other aspects of the school's life.

3) Developing Academic Potential

a) The National Curriculum provides the basic framework. It, is delivered through - Schemes of Work, teaching and learning styles, assessment procedures, Special Needs Support, the Learning Support Unit, the Gifted & Talented Programme and cross-curricular themes.

2. Purpose

2.1 To ensure that the use if ICT within the school by staff, students, parents\carers and governors, meets the legal framework of supporting the "The Green Paper *Every Child Matters*" and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children* which sets out how the school and individuals should work together to safeguard and promote the welfare of children.

2.2 The 'staying safe' outcome includes aims that children and young people are:

i. safe from maltreatment, neglect, violence and sexual exploitation
ii. safe from accidental injury and death
iii. safe from bullying and discrimination
iv. safe from crime and anti-social behaviour in and out of school
v. Secure, stable and cared for.

Through this policy we aim to adopt an e-safety environment for all users.
It is the duty of the school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

3. The technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

1 The Internet
2 e-mail
3 Instant messaging (http://www.msn.com, http://info.aol.co.uk/aim/) often using simple web cams
4 Blogs (an on-line interactive diary)
5 Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
6 Social networking sites (Popular www.myspace.com / www.piczo.com / www.bebo.com / http://www.hi5.com / http:www.facebook.com)
7 Video broadcasting sites (Popular: http://www.youtube.com/)
8 Chat Rooms (Popular www.teenchat.com, www.habbohotel.co.uk)
9 Gaming Sites (Popular www.neopets.com, http://www.miniclip.com/games/en/, http://www.runescape.com/ / http://www.clubpenguin.com)
10 Music download sites (Popular http://www.apple.com/itunes/ http://www.napster.co.uk/ http://www-kazzaa.com/, http://www-livewire.com/)
11 Mobile phones with camera and video functionality
12 Mobile technology (e.g. games consoles) that are 'internet ready'.
13 Smart phones with e-mail, web functionality and cut down 'Office' applications.

4. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

1 An effective range of technological tools;

2 Policies and procedures, with clear roles and responsibilities;

3 A comprehensive e-Safety education programme for students, staff and parents\carers.

Ref: Becta - E-safety Developing whole-school policies to support effective practice

5. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head teacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the Communication Information Systems Manager who is supported by a member of the senior leadership team.

Our school **e-Safety Co-ordinator** is the Communication Information Systems Manager (CIS MAN)

Our e-Safety Coordinator ensures he/she keeps up to date with e-Safety issues and guidance through liaison with the Local Authority e-Safety Officer and through organisations such as Becta and The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinator ensures the Head Teacher, senior leadership and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.
All teachers are responsible for promoting and supporting safe behaviour in their classrooms and following school e-Safety procedures.

Central to this is fostering a 'No Blame' culture so students, staff, parents/carers and governors feel able to report any bullying, abuse or inappropriate materials.
All staff should be familiar with the schools' Policy including:

1. Safe use of e-mail;
2. Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
3. Safe use of school network, equipment and data;
4. Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
5. publication of student information/photographs and use of website;
6. e-Bullying / Cyber bullying procedures;
7. their role in providing e-Safety education for students;

Staff are reminded / updated about e-Safety matters at least once a year.
St Ursula's Convent School will include e-safety in the curriculum and ensure that every student has been educated about safe and responsible use. Students need to know how to control and minimise online risks and how to report a problem.

St Ursula's Convent School will ensure that they make efforts to engage with parents\carers over e-safety matters and those parents/carers have signed and returned an e-safety/AUP form.

6. Communications

How will the policy be introduced to students?

Disseminate: Many students are very familiar with the culture of new technologies, and the School e-Safety Policy is discussed via the student council, at assemblies and during citizenship days. Students' perceptions of the risks may not be mature; so the e-safety rules will be explained or discussed. In addition to this, students are taught about e-safety during their ICT lesson time. Students also sign an acceptable user's agreement. This information forms is included in the transition/admission documentation.

How will the policy be discussed with staff?

Disseminate: It is important that all staff feel confident to use new technologies in teaching. Staff are given opportunities to discuss the issues and develop appropriate teaching strategies in subject area meetings, full staff meetings and Central leaders meeting.

Staff must understand and fully accept the procedure for information systems misuse. If a member of staff is concerned about any aspect of their ICT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

ICT use is widespread and all staff including administration, premises, governors and other support staff are included in appropriate awareness raising and training. Induction of new staff includes a discussion of the school's e-Safety Policy.

Issues that staff must be aware of:

- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

How will parents\carers support be enlisted?

- **Disseminate:** Internet use in students' homes is increasing rapidly. The school will communicate issues regarding e-safety to parents\carers via letters, contact and at the annual curriculum evenings and where possible demonstrations will be provided. The school will provide advice on filtering systems and educational and leisure activities that include responsible use of the Internet.

7. How will complaints regarding e-Safety be handled?

St Ursula's Convent School will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that

unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Parents/Carers, staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

1 interview/counselling by Form tutor / Head of Department / Key Stage Learning Manager / e-Safety Coordinator / Deputy Head or the Head teacher;
2 informing parents or carers;
3 removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
4 Referral to Local Authority / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint about staff misuse which is then referred to the Head teacher.

For student complaints subject teachers must refer the matter to the E-safety coordinator.

Complaints of cyber bullying (within school) are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with the school child protection procedures.

8. Guidance: What do we do if?

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the Head teacher/e- safety officer and decide whether to inform parents\carers of any children who viewed the site.
3. Inform the IT technicians and ensure the site is filtered report to: **webalerts@synetrix.com**).
4. Inform the Local Authority if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
2. Notify the parents\carers of the child.
3. Inform the IT technicians and ensure the site is filtered if need be.
4. Inform the Local Authority if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. If a member of staff finds anything inappropriate this must be reported immediately to the Head teacher.
2. Ensure you have a colleague with you; do not view the misuse alone.
3. Report the misuse immediately to the Head teacher and ensure that there is no

further access to the PC or laptop.

4. If the material is offensive but not illegal, the Head teacher should then:
    1 Remove the PC to a secure place.
    2 Instigate an audit of all IT equipment by the school's IT managed service providers to ensure there is no risk of students accessing inappropriate materials in the school.
    3 Identify the precise details of the material.
    4 Take appropriate disciplinary action (contact Personnel/Human Resources).
    5 Inform governors of the incident.
4. In an extreme case where the material is of an illegal nature:
    1 Contact the local police or High Tech Crime Unit and follow their advice.
    2 If requested to remove the PC to a secure place and document what you have done.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.

1. Advise the child not to respond to the message.
2. Refer to relevant policies including e-safety, anti-bullying and Child protection and apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's e-mail service provider.
5. Notify parents\carers of the children involved.
6. Inform the police if necessary.
7. Inform the Local Authority e-safety officer, if appropriate

Malicious or threatening comments are posted on an Internet site about a student, member of staff or the school.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform Local Authority e-safety officer, if appropriate

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child

1. Report to and discuss with the named child protection officer in school and contact parents\carers.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and social services.
5. Inform Local Authority e-safety officer, if appropriate
6. Consider delivering a parent\carers workshop for the school community, if

appropriate.

All of the above incidences must be reported immediately to the Head teacher, E-safety officer or the Child Protection Officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

9. Technical and Infrastructure Policy

The school:

1 Maintains the filtered broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
2 Works in partnership with the Local Authority to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
3 Has additional user-level filtering in-place using the Synetrix Service
4 Ensures network health through appropriate anti-virus software etc and network set-up so staff and students cannot download executable files such as .exe / .com / .vbs etc.;
5 Ensures their network is 'healthy' by having health checks annually on the network;
6 Utilises caching as part of the network set-up;
7 Ensures the IT Team are up-to-date with LGfL services and policies;
8 Ensures the IT Team checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
9 Never allows students access to Internet logs;
10 Has Ranger network auditing software installed;
11 Uses individual log-ins for students and all other users;
12 Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
13 Never sends personal data over the Internet unless it is encrypted or otherwise secured;
14 Never allows personal level data off-site unless it is on an encrypted device or otherwise secured.
15 Uses 'safer' search engines with students such as http://yahooligans.yahoo.com/ | http://www.askforkids.com/ and activates 'safe' search where appropriate;
16 Ensures students only publish within appropriately secure learning environments such as their own closed secure LGfL portal or Learning Platform.

10. **Internet Policy and procedures:**

The school:

1 Supervises students' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older students have more flexible access;
2 We use the pan-London LGfL / Synetrix filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
3 Staff preview all sites before use or only use sites accessed from managed 'safe' environments such as the Learning Platform;
4 Plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required;
5 Never allows / Is vigilant when conducting 'raw' image search with students e.g. Google or Lycos image search;
6 Informs users that Internet use is monitored;
7 Informs staff and students that that they must report any failure of the filtering systems directly to the IT Team and report to Local Authority / LGfL if appropriate.
8 Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
9 Only unblocks social networking sites for specific purposes / Internet Literacy lessons; however the school may not be able to do this because of the LA filtering system.
10 Only uses the LGfL / NEN service for video conferencing activity;
11 Only uses approved or checked webcam sites;
12 Has blocked student access to music download or shopping sites – except those approved for educational purposes.
13 Requires students (and their parent/carer) from Key Stage 3 and 4, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
14 Uses closed / simulated environments for e-mail with students;
15 Requires all staff to sign an e-safety / acceptable use agreement form and keeps a copy on file;
16 Makes clear that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
17 Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
18 Ensures the named child protection officer has appropriate training;
19 Ensures parents\carers provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their daughter's entry to the school;
20 Makes information on reporting offensive materials, abuse / bullying etc. available for students, staff and parents\carers;
21 Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the Local Authority.

11. Education and training Policy for staff delivering ICT across the school

This school:

1. Fosters a 'No Blame' environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
2. Ensures students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or IT Technical team.
3. Ensures students and staff know what to do if there is a cyber-bullying incident;
4. Ensures all students know how to report abuse;
5. Has a clear, progressive e-safety education programme throughout all Key Stages, built on Local Authority / national guidance. Students are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand 'Netiquette' (protocol for using the internet) behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;

6 Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;

7 Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

8 Makes training available annually to staff on the e-safety education program;

9 Runs a rolling programme of advice, guidance and training for parents\carers, including:

- Information in school newsletters; on the school web site;
- demonstrations, practical sessions held at school, if requested
- distribution of 'think u know' for parents\carers materials
- suggestions for safe Internet use at home;
- Provision of information about national support sites for parents\carers.

12. E-mail Policy:

This school:

1 Does not publish personal e-mail addresses of students or staff on the school website. We use anonymous or group e-mail addresses.

1 If one of our staff or students receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.

2 Accounts are managed effectively, with up to date account details of users

3 Messages relating to or in support of illegal activities may be reported to the authorities.

4 Spam, phishing and virus attachment can make e-mail dangerous. Use filtering software to stop unsuitable mail, LGfL emails reject 9 out of 10 emails received.

Students:

5 Students can only use the school's internal web based e-mail system

6 Students are introduced to, and use e-mail as part of the ICT scheme of work.

7 Students are taught about the safety and 'netiquette' (protocol for using the internet) of using e-mail i.e.

- not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/career;
- that an e-mail is a form of publishing where the message should be clear, short and concise;

- that any e-mail sent to an external organization should be written carefully and authorized before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- the sending of attachments should be limited;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages,
- not to delete malicious or threatening e-mails, but to keep them as evidence of bullying;
- not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding 'chain' e-mail letters is not permitted;

8 Students sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

9 Staff use Outlook or web outlook e-mail systems for professional purposes;

10 Access in school to external personal e-mail accounts may be blocked;

11 That e-mail sent to an external organization is written carefully, (and may require authorization), in the same way as a letter written on school headed paper. That it should follow the school 'house-style';

- the sending of attachments should be limited;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

12 Staff signs the appropriate school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

13. Policy: Managing Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

Policy / Procedure statements:

To ensure the network is used safely this school:

1 Ensure staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;

2 Provides students with an individual network log-in username and password

3 Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;

4 Makes clear that students should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;

5 Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;

6 Has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;

7 Requires all users to always log off when they have finished working or are leaving the computer unattended;

8 Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.

9 Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day / we automatically remotely switch off all computers at 8 o'clock;

10 Has set-up the network so that users cannot download executable files / programmes;

11 Has blocked access to music download or shopping sites – except those approved for educational purposes;

12 Scans all mobile equipment with anti-virus / spyware before it is connected to the network;

13 Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;

14 Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.

15 Maintains equipment to ensure Health and Safety is followed;

16 Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
e.g. teachers access report writing module; SEN coordinator - SEN data

17 Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAS system;

18 Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
e.g. technical support or SIMS Support through LA systems; Education Welfare Officers accessing attendance data on specific children, parents\carers using a secure portal to access information on their child.

19 Provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their FRONTER username and password.

20 Uses our broadband network for our CCTV system and this has been set-up by approved LGfL partners;

21 Uses the DfES secure s2s website for all CTF files sent to other schools;

22 Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;

23 Reviews the school ICT systems regularly with regard to security.

14. Policy: How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Head Teacher.

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

*[Sanctions: **referred to class teacher / Form Tutor** / **senior leader / e-Safety Coordinator,** restriction of rights or withdrawal of internet access and/or Learning Platform access rights for a period]*

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chat rooms, social networking sites, Newsgroups
- Use of File sharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Sanctions: ***referred to Class teacher/ subject leader / HOD / KS Learning Manager / e-safety Coordinator*** */ removal of Internet access rights and/or Learning Platform access rights for a period of time / contact with parent*\carers*, exclusion]*

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Sanctions: ***referred to Class teacher / HOD / KS Learning Manager / E-safety Coordinator / Head teacher /*** *removal of Internet and/or Learning Platform access rights for a period / contact with parents\carers \ removal of equipment, exclusion]*

Other safeguarding actions

If inappropriate web material is accessed:

- Ensure appropriate technical support filters the site
- Inform Local Authority / Synetrix as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

*[Sanctions – **Referred to Head Teacher / Contact with parents/carers** / exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer]*

Other safeguarding actions:

- Secure and preserve any evidence
- Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the World Wide Web that compromises the staff member's professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network or local machines.

*[Sanction - **referred to line manager / Head teacher**. Warning given.]*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to any school computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*[Sanction – **Referred to Head teacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of students accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The School will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the Head Teacher will **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

1. They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
2. Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Students will sign an appropriate e-safety / acceptable use form;
3. The school's e-safety policy will be made available and explained to parents\carers, and parents\carers will sign an acceptance form when their child starts at the school.
4. Information on reporting abuse / bullying etc. will be made available by the school for students, staff and parents\carers
5. Staff are issued with the 'What to do if?' guide on e-safety issues.

15. MONITORING AND REVIEW

15.1 This policy will be monitored by the Deputy Head and the Communication Information Systems Manager who will report to the Head teacher on its implementation on a regular basis.

15.2 The Head teacher will report to the governing body's Curriculum Committee on the progress of the policy and will recommend any changes.

15.3 All new staff, parents\carers and students will sign an AUP contract on entry into the school.

Acceptable Use Policy (AUP): Parents/carers Contract

(Refer to ICT Policy)

Student name(s): …… Reg Group ……
(Please print name)

Student name(s): …… Reg Group ……
(Please print name)

As the parent or legal guardian of the above student(s), I grant permission for my daughter to have access to use the Internet, e-mail and other ICT facilities at school.

I know that my daughter has signed an e-safety agreement form and that they have a copy of the 'rules for responsible ICT use'.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail*, employing appropriate teaching practice and teaching e-safety skills to students.

I understand that the school can check my child's computer files, and the Internet sites they visit and that if they have concerns about their e-safety or e-behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

Parent\Carers Name: _____
(Please print name)

Parent / Carer signature: _____

Date: ___/___/___

Useful e-safety programmes include:

1. Think U Know; currently available for secondary students. http://www.thinkuknow.co.uk
2. Grid Club http://www.gridclub.com/
3. The BBC's Chat Guide: http://www.bbc.co.uk/chatguide/

Acceptable Use Policy (AUP): Staff Contract (Inc. Supply)

(Refer to ICT Policy)

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

1 I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

2 I will only use the approved, secure email system(s) for any school business (currently Outlook web-mail).

3 I will not browse, download, create, store or send material that could be considered offensive, pornographic, obscene, suggestive, menacing or harassing to another person

4 I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / CIS Manager.

5 I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.

6 I will not share or provide my username and password to anyone.

7 I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

8 I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

9 I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.

10 I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended system.

11 I will not use personal digital cameras or camera phones for transferring images of students or staff without permission.

12 I will use the school's Learning Platform in accordance with school advice.

13 I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role, or adversely affect the reputation of the school and follow the guidance set up by Greenwich HRS. Privacy on social networking sites will be of the highest level to safeguard staff, students and the school.

14 I will not engage in any online activity that may compromise my professional responsibilities.

15 I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that any damage, loss or theft is the responsibility of the staff member; which should be reported to the Head Teacher/ IT technical team. I will notify the school of any "significant personal use" as defined by

HM Revenue & Customs.

16 I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

17 I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. The transfer of personal student information is forbidden unless authorised by the Head Teacher. E.g. addresses.

18 I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.

19 I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …….…… Date ……

Full Name ……..... (Printed)

Job title . . . . . .

School . . . . . .

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature ……..... Date ……

Full Name ……..…. (Printed)

Acceptable Use Policy (AUP): Student Contract

(Refer to ICT Policy)

This document outlines St Ursula's Convent School policy in relation to the use of IT equipment and systems. The policy has been constructed after reviewing best practice use and the relevant legislation currently in force. It seeks to clarify what the school regards as acceptable and unacceptable use and it is designed to ensure that we meet all legal requirements, minimise our exposure to risk, protect our information and utilise the equipment in the most effective manner.

You will be asked to read the following rules listed below and to sign this Acceptable Use Contract.
If you fail to follow these rules you could cause the school significant problems and expense.
Only those students who return a signed contract will be allowed to use the computers.

All students should understand that the school has software that can track **all** Internet and non Internet use i.e. the use of Word and other documents and recognises words and phrases that Should not be used on its PCs. Individuals **will** be held to account for inappropriate material or Words and phrases that appear under that person's user log on details.

1. The Rules

2. Do not enter any computer room unless a member of staff is present.

3. When you "log on" make sure you only ever use your own password and personal login code. Never let any other person know your password or use your code.

4. You are only allowed to use the software you can see on the "menus or icons" which appear on the screen. Using any "hidden" computer programs or "hacking" is not allowed.

5. There are no other programmes/games allowed anywhere on the network, and none should be brought into school or downloaded from the Internet.

6. Do not input/download/view anything obscene or offensive onto any school computer or other user area at any time i.e. to or from the Internet or by any other means.

7. Log out properly. If you are not able to return to the log on screen only turn off the computer with a member of staff's permission.

8. If you find that your computer is faulty, has no mouse, keyboard etc, please inform your teacher and they will inform the ICT Technician. Do not try to disconnect anything as you could cause a lot of damage to the connectors and you may have to pay for any repairs for damage caused.

9. Do not touch the cables or wires at the back of the computer or the computer points attached to the walls, as this could be extremely dangerous. If you have a problem with any of these items, please see a member of staff immediately.

10. If you are required to bring discs, USB devices or the like from home into the school please take them to the IT technician or an ICT teacher to check the disc, USB devices or the like for viruses. Do not use discs that have not been virus checked on the system at any time.

11. Any misuse or actions using the technologies which bring the school into disrepute will lead to sanctions in accordance with the school's behaviour/discipline policy.

12. Any misuse or inappropriate actions using the technologies which cause offence to staff and other students will lead to sanctions in accordance with the school's behaviour/discipline policy.

13. Food and drink can cause damage to the computers and should **never** be brought into computer rooms.

14. Any incidents where the above rules are not followed could result in immediate suspension from the network. Depending on the severity of the offence a range of sanctions may be applied in accordance with the school's Discipline /Behaviour Policy, i.e. being in a computer room without a member of staff could result in a detention; "Hacking" could result in being taken off the network for a significant period of time. Second or third offences could lead to permanent suspension from the network or to more serious sanctions given.

15. Any acts of proven vandalism will result in parents\carer being required to come into school as part of a full investigation. Bills for repairs will also be issued.

Remember: you are responsible for anything found on your user area.
Don't find yourself logged off the Network/Internet because any of the above rules have been broken.

If you do not understand any of these rules please ask your ICT teacher or an IT technician or any other member of staff to explain them to you.

Once this document has been signed, please return it to your tutor as soon as possible.

A copy of this document will be given to you once the school has received the signed copy

Student forename _____ **Student surname** _____

Student Signature _____ **Reg Group** _____

Date_____

Acceptable Use Policy (AUP): Governors Contract

(Refer to ICT Policy)

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

1. I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
2. I will use an approved, secure email system(s) for any school business.
3. I will not browse, download, create, store or send material that could be considered offensive, pornographic, obscene, suggestive, menacing or harassing to another person.
4. I will report any accidental access to, or receipt of inappropriate materials, to the Head Teacher.
5. I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
6. I will not download any software or resources from the Internet that can compromise the school.
7. I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
8. I will not use personal digital cameras or camera phones for transferring images of students or staff without permission.
9. I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role, or adversely affect the reputation of the school and follow the guidance set up by Greenwich HRS. Privacy on social networking sites will be of the highest level to safeguard staff, students and the school.
10. I will not engage in any online activity that may compromise my professional responsibilities relating to the school.
11. I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that any damage, loss or theft is the responsibility of the staff member; which should be reported to the Head Teacher/ IT technical team. I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
12. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
13. I understand that data protection policy requires that any information seen by me with regard to staff, parent\carer or student information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an

appropriate authority. The transfer of personal student information is forbidden unless authorised by the Head Teacher.

14. I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy (normally an annual revisit).

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …….…… Date …….

Full Name ……..... (Printed)

Job title . . . . . .

School . . . . . .

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature …….…….... Date …….

Full Name ……..…. (Printed)