ICS
icschool.co.uk

ICT POLICY INCORPORATING E-SAFETY
(Whole School)

1. Rationale

1.1 Teaching and learning 2

2 School e-safety strategies

2.1 Risks 3
2.2 Roles and responsibilities 4
2.3 students with special needs 7
2.4 Working with parents 7

3 E-safety policies

3.1 Access to and monitoring of systems 8
3.2 Acceptable use policies 8
3.3 Teaching e-safety 9
3.4 ICT and safe teaching practice 10
3.5 Safe use of ICT 11

4 Responding to incidents

4.1 Policy statement 17
4.2 Unintentional access by students
17
4.3 Intentional access by students 18
4.4 Inappropriate ICT use by staff 18
4.5 Cyberbullying 19
4.6 Inappropriate contacts 21

4.7 Violent extremism on the internet 22

5 Sanctions for misuse of ICT

5.1 students 23
5.2 Staff 35

Appendices:

Appendix 1: Acceptable use policies for primary schools 27
Appendix 2: Acceptable use policies for secondary schools 29
Appendix 3: Acceptable use policies for staff 31
Appendix 4: E-safety incident report form 33
Appendix 5: Netbook loan agreement and charter

1. RATIONALE

ICS understands the great power inherent in modern technology and appreciates that a truly connected world can only exist through harnessing technology. We realise that it is our duty to take responsibility for the safety and appropriate use of technology in our organisation and in the life of its members. Our starting point with our students, which is reinforced through the education provided at ICS, is that they understand where the boundaries of appropriate uses of technology lie and in which cases they might be vulnerable to inappropriate online content, contact and/or conduct. Respecting others is at the heart of our philosophy and extends into the digital domain. These boundaries however are changing as familiarisation with new forms of communication develop. With our selected bring your own device (BYOD) system, we create the opportunity for our students to learn about different devices and how each device comes with its strengths and vulnerabilities.

ICS recognises that the Internet and other digital technologies provide a vast opportunity for children and young people to learn. The Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, collaboration, stimulate global awareness, teach online safety and resilience and to enhance the learning experience.

As part of our commitment to learning and achievement in a safe environment, we at ICS want to ensure that the Internet and other digital technologies are used to:

- raise educational standards and promote student achievements;
- develop the curriculum and make learning exciting and purposeful;
- enable students to gain access to a wide span of knowledge in a way that ensures their safety and security;
- develop students' skills of cooperation, collaboration, resilience and competition;
- prepare our students to be effective 21st century citizens.
- train and educate our staff, students and parent community about the appropriate use of online technologies and risks to their safety.

The school's ICT policy will operate in conjunction with other policies including those for Student Behaviour and Sanctions, Child Protection and Curriculum.

1.1. Teaching and learning

1.1.1. Why Internet use is important

The Internet is an essential element in 21st century life for education, collaboration, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the curriculum and a necessary tool for staff and students.

1.1.2. Internet use enhances learning

The school Internet access is designed expressly for staff and student use and includes filtering appropriate to the age of students.

Students are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2. School E-safety strategies

2.1. Risks

The risk associated with use of ICT by children can be grouped into 4 categories.

2.1.1. Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

2.1.2. Contact

Chat rooms and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children’s trust (known as “grooming”) with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as cyber bullying. More details on this can be found in our Cyber Bullying section.

2.1.3. Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.

2.1.4. Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, antisocial or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- using information from the internet in a way that breaches copyright laws
- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience
- cyber bullying.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.

2. 2. Roles and responsibilities

A successful e-safety strategy needs to be inclusive of the whole school community and forge links with parents and carers. The strategy should be overseen by the Head of Schools, ICT co-ordinators and be fully implemented by all staff, including technical and non-teaching staff.

2.2.1. School Heads' role

School Heads have ultimate responsibility for e-safety issues within the school including:

- the overall development and implementation of the school's e-safety policy
- ensuring that e-safety issues are given a high profile within the school community
- linking with the senior management, parents and carers to promote e-safety and forward the school's e-safety strategy

- ensuring e-safety is embedded in the curriculum
- deciding on sanctions against staff and students who are in breach of acceptable use policies.

2.2.2. E-safety officer / ICT coordinator's role

Both schools (Primary and Secondary) have a designated e-safety contact officer who is responsible for co-ordinating e-safety policies on behalf of the school. Given the issues associated with e-safety, it is appropriate for the child protection officer/DSPs to be working alongside the school's e-safety officers.

The e-safety officers have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's e-safety policy
- ensure that staff and students are aware that any e-safety incident should be reported to them
- provide the first point of contact and advice for school staff, governors, students and parents
- liaise with the school's Network Administrator to ensure they are kept up to date with e-safety issues and to advise of any new trends, incidents and arising problems to the head teacher
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and the Schools IT teams
- raise the profile of e-safety awareness with the school by ensuring access to training and relevant e-safety literature
- ensure that all staff and students have read and signed the acceptable use policy (AUP)
- report annually to the heads of school on the implementation of the school's e-safety strategy
- maintain a log of internet related incidents and co-ordinate any investigation into breaches
- carrying out monitoring and audits of networks and reporting breaches to the e-safety officers.

2.2.3. Network Administrator's role

The role of the Network administrator:

- the maintenance and monitoring of AVG and Webroot, including antivirus and URL filtering systems.
- supporting any subsequent investigation into breaches and preserving any evidence.

2.2.4. Role of school staff

Teaching staff have a dual role concerning their own internet use and providing guidance, support and supervision for students. Their role is:

- adhering to the school's e-safety and acceptable use policy and procedures
- communicating the school's e-safety and acceptable use policy to students
- keeping students safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the e-safety officer
- recognising when students are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the e-safety officer.

2.2.5. Designated Senior Person/DSP

Where any e-safety incident has serious implications for the child's safety or well-being, the matter should be referred to the designated DSP for the school who will decide whether or not a referral should be made to Safeguarding and Social Care or the Police.

2.3. Students with special needs

students with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision.

SEN co-ordinators are responsible for providing extra support for these students and should:

- link with the e-safety officer to discuss and agree whether the mainstream safeguarding systems are adequate for students with special need.
- where necessary, liaise with the e-safety officer and the Schools IT team to discuss any requirements for further safeguards or tailored resources and materials in order to meet the needs of students with special needs
- ensure that the school's e-safety policy is adapted to suit the needs of students with special needs.
- liaise with parents, carers and other relevant agencies in developing e-safety practices for students with special needs
- keep up to date with any developments regarding emerging technologies

and e-safety and how these may impact on students with special needs.

2.4. Working with parents and carers

It is essential that schools involve parents and carers in the development and implementation of e-safety strategies and policies; most children will have internet access at home and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The principals and the e-safety officers should consider what strategies to adopt in order to ensure parents are aware of e-safety issues and support them in reinforcing e-safety messages at home.

Parents should be provided with information on ICT learning and the school's e-safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour.

3 E-SAFETY POLICIES

3.1 Accessing and monitoring the system

- Access at primary level is on individual basis for each student with a netbook; for secondary school students if they use a school netbook are able to set their own passwords, staff access is through departmental logins and passwords as well as school netbooks. (See netbook policies)

- ICS primary netbook programme. Students in Years 3-6 take part in the ICS netbook programme where each student is assigned a personal netbook connected to our wireless network. Student netbooks are installed with educational software including Movie Maker, Microsoft Office, Scratch, Google Earth, etc. Netbooks are integrated daily in teaching and learning throughout Years 3-6.

  Parents of students in Years 3-6 must sign user contracts when netbooks are issued. These contracts outline terms and conditions, including responsibility for lost, broken netbooks, etc. (see Appendix 5)

  Other forms of technology devices used to enhance the Primary Years Programme include iPads, laptops and PCs. Students have shared access to these tools in class under teacher guidance.

- ICS Secondary adopts a 'Bring Your Own Device' scheme whereby students are encouraged to bring their own devices to use in school coupled with the ICS netbook programme. We believe that greater learning is achieved through the negotiation of different devices collaborating to complete the same work. Minimum requirements are sent to parents to make sure that students bring devices that can do the work that is necessary and devices that conform with current network standards.

Student netbooks are installed with educational software including Movie Maker, Microsoft Office, Scratch, Google Earth, etc.

Parents of students using netbooks must sign user contracts when netbooks are issued. These contracts outline terms and conditions, including responsibility for lost, broken netbooks, etc. (see Appendix 5)

Other forms of technology devices used to enhance the Secondary Programme include class sets of iPads and teacher desktop PCs.

- The school takes no responsibility for the damage of personal devices. The same conduct use terms that apply to school netbooks also apply to personal devices.

- The e-safety officer has access to all netbooks and can access all log-ins used within the school for the purposes of monitoring and auditing internet activity.

- Network administrator and e-safety officers responsible for monitoring systems are supervised by heads of schools.

3.2 Acceptable use policies

- All netbook users and BYOD users within the school will be expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates the school e-safety rules regarding their internet use.

- For Primary school students, acceptable use agreements will be signed by parents on their child’s behalf at the same time that they give consent for students to access the internet via netbooks. (see appendix 6 for current netbook loan charter and appendix 1 for acceptable use policy for Sep 2014).

- Secondary school students and their parents should both sign the acceptable use policy, and use of ICS IT provision in schools is dependent on signing this agreement (see appendix 2 start Sep 2014).

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 3).

The e-safety officers will keep a copy of all signed acceptable use agreements.

3.3 Teaching e-safety

3.3.1 Responsibility

One of the key features of the school's e-safety strategy is teaching students to protect themselves and behave responsibly while online. There is an expectation that over time, students will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

Overall responsibility for the design and coordination of e-safety education lies with the Head of Schools and the e-safety officers, but all teaching staff should play a role in delivering e-safety messages. The e-safety officers are responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

EXAMPLES OF STRATEGY IN ACTION
E-citizenship (Primary)
Appropriate online conduct will be modelled by teachers and regularly integrated into primary units of inquiry.

Lessons and activities from the 'Common Sense Media Digital Citizenship and Literacy' classroom curriculum will reinforce online safety awareness in an age-appropriate way.

Students in Years 3-6 will create Digital Citizenship Pledges that outline an online code of conduct they agree to follow.

E-safety training opportunities for staff, students and parents using visiting experts and school resources support strategy development.

E-Resilience (Secondary)
Appropriate online conduct is modelled by teachers who regularly use online resources for teaching.

Technology teaching at MYP level incorporate an aspect of e-resilience in each unit of learning.
For the Diploma students online positive virtual reputation is integrated into English lessons giving students the opportunity to create content online that will promote their employability.

PSHE lessons using the 'Common Sense Media Digital Citizenship and Literacy' programme are used to inform students about the risks and rewards of the online world covering an array of topics that are described below.

E-safety training opportunities for staff, students and parents using visiting experts and school resources support strategy development.

3.3.2 Content

students are taught:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that the school has a “no blame” policy so that students are encouraged to report any e-safety incidents
- that the school has a “no tolerance” policy regarding cyber bullying
- behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action
- School internet should only be used for educational purposes
- The school system has been designed so that use is monitored and that access to some sites are blocked
- the school’s policy on using their own mobile phones whilst in school.

3.3.3 Delivering e-safety messages

- Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use are posted around the school to make students aware of any risks and reporting protocols.

- The start of every lesson where computers are being used should be an opportunity to remind students of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers use PSHE lessons as a forum for discussion on e-safety issues to ensure that students understand the risks and why it is important to regulate their behaviour whilst on-line.

- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

- Teachers should ensure that the school’s policy on students’ use of their own mobile phones in school is adhered to.

- Safer internet day contributes to highlighting internet safety to all students and staff.

3.4 ICT and safe teaching practice

ICS staff are made aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with students.

The following points should be followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of students should only be taken by staff in connection with educational purposes.

- Staff should only store images on the school computer system, with all other copies of the images erased.

- Staff should take care regarding the content of and access to their own social networking sites and ensure that students and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff should be particularly careful regarding any comments to do with the school or specific students that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff should not engage in any conversation with students via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with students regarding school work, this should be via school email or Managebac and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or students by telephone, staff should only use school equipment. student or parent numbers should not be stored on a staff member’s personal mobile phone and staff should avoid lending their mobile phones to students.

- Staff should ensure that personal data relating to students is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.

3.5 Safe use of ICT

3.5.1 Internet and search engines

- When using the internet, students should receive the appropriate level of supervision for their age and understanding. Teachers should be aware that often, the most computer-literate children are the ones who are most at risk.

- Primary school children should be supervised at all times when using the internet. Although supervision of secondary school students will be more flexible, teachers should remain vigilant at all times during lessons.

- students should not be allowed to aimlessly “surf” the internet and all use should have a clearly defined educational purpose.

- Despite filtering systems, it is still possible for students to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the e-safety officer, who will liaise with the Network Administrator for temporary access. Teachers should notify the e-safety officer once access is no longer needed to ensure the site is blocked.

3.5.2 Evaluating and using internet content

As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach students good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:

- questioning the validity of the source of the information; whether the author’s view is objective and what authority they carry

- carrying out comparisons with alternative sources of information

- considering whether the information is current and whether the facts stated are correct.

In addition, students should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying others work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

3.5.3 Emails

ICS makes use of Gmail to communicate with staff and students. Managebac is also be used to send messages to students.

- Access to and use of personal email accounts on the school intranet is forbidden. This is to protect students from receiving unsolicited mail and preserve the safety of the system from hacking and viruses.

- Emails should only be sent via Gmail for professional and educational purposes only.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the e-safety contact officer who will liaise with the Schools IT team.

- students should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.

- All email communications should be polite; if a student receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.

- students should be warned that any bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- Users should be aware that as use of e-mail via mail.ics.uk.net is for the purposes of education or school business only, and all emails may be monitored.

- Primary and secondary school students should be issued with an individual account using their log-in and password.

- All email messages sent by students in connection with school business must be checked and cleared by the responsible teacher.

- Apart from the headteacher, marketing manager and administrator, individual email addresses for staff or students should not be published on the school website.

- students should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

3.5.4 Social networking sites, newsgroups and forums

Social networking sites such as Facebook, Twitter and Tumblr allow users to publish information about them to be seen by anyone who has access to the site. The use of these sites are not prohibited in ICS, but is not to be used during class time.

Newsgroups and forums are sites that enable users to discuss issues and share ideas online. Some schools may feel that these have an educational value.

- Access to unregulated public social networking sites, newsgroups or forums are blocked by the school filter.

- Where schools identify a clear educational use for these sites for online publishing, they should only use approved sites allowed by the school filter and professional judgement should be used.

- Any use of these sites should be strictly supervised by the responsible teacher.

- students should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

- In order to teach students to stay safe on social networking sites outside of school, they should be advised:
    - not to give out personal details to anyone online that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended

    - not to upload inappropriate or revealing personal photos of themselves or others onto sites and to take care regarding what information is posted

    - how to set up security and privacy settings on sites or use a “buddy list” to block unwanted communications or deny access to those unknown to them

    - to behave responsibly whilst on-line and keep communications polite

    - not to respond to any hurtful or distressing messages but to let their parents, carers or e-safety contact officer know so that appropriate action can be taken.

3.5.5 Chat rooms and instant messaging

Chat rooms are internet sites where users can join in “conversations” online ; instant messaging allows instant communications between two people on-line. In most cases, students will use these at home although the school filter does block some of these applications.

- Inappropriate or adult chat rooms are blocked by the school filter, but instant messaging apps are mostly not blocked on student’s personal devices.

- students should be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated and will be dealt with in accordance with the school’s anti-bullying policy.

- In order to teach students to stay safe whilst using chat rooms outside of school, they should be advised:

    - not to give out personal details to anyone online that may help to identify or locate them or anyone else (disable geo positioning)

    - only use moderated chat rooms that require registration and are specifically for their age group

    - not to arrange to meet anyone whom they have only met online

    - to behave responsibly whilst on-line and keep communications polite

    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

3.5.6 Video conferencing

Video conferencing enables users to communicate face-to-face via the internet using web cameras.

- Video conferencing during school time should only be used for professional purposes.

- Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the Schools IT team.

- student use of video conferencing should be for educational purposes and should be supervised as appropriate to their age. students must ask permission from the responsible teacher before making or receiving a video conference call.

- Teachers should ensure that students are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.

- Photographic or video devices may be used by teachers only in connection with educational activities including school trips.

- Photographs and videos may only be downloaded onto the school's computer system with the permission of the network manager and should never enable individual students' names or other identifying information to be disclosed.

3.5.7 School website

- Content should not be uploaded onto the school website unless it has been authorised by the e-safety contact officer and the headteacher, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- The marketing manager and school administrator have responsibility for uploading materials onto the school website.

- To ensure the privacy and security of staff and students, the contact details on the website should be the school address, email and telephone number. No contact details for staff or students should be contained on the website.

- Children's full names should never be published on the website.

- Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

3.5.8 Photographic and video images

- Where the school uses photographs and videos of students for publicity purposes, for example on the school website, images should be carefully selected so that individual students cannot be easily identified. It is recommended that group photographs are used.

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.

- Children’s names should never be published where their photograph or video is being used.

- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images should be securely stored only on the school’s computer system and all other copies deleted. If personal equipment is used to take videos or images of students the content needs to be deleted from the staff members equipment before leaving the school at the end of the day. For ongoing projects where film or images are involved staff are encouraged to make use of school filming or camera equipment. Any exceptions to this rule must be discussed with the school principal.

- Stored images should not be labelled with the child’s name and all images held of children should be deleted once the child has left the school.

3.5.9 students own mobile phone/handheld devices

The majority of students are likely to have mobile phones or other equipment that allows them to access internet services, and these can pose a major problem for schools in that their use may distract students during lessons and may be used for cyber bullying.

However, many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to.

At ICS the use of mobile phones during class is forbidden unless a teacher gives direct permission. Calls from parents are not allowed to be answered during class times and emergency calls should be made via the reception desk.

Students are allowed to use their tablets for school work and need to comply to the acceptable use policy.

Mobile device zones are sign posted around the school to indicate where students are able to use their mobile devices during break and lunch times. Students and teachers are not allowed to take any photos in or around the toilets.

4 RESPONDING TO INCIDENTS

4.1 Policy statement

- All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the e-safety officer in the first instance. All incidents, whether involving students or staff, must be recorded by the e-safety officer on the e-safety incident report form (appendix 4).

- Where the incident or complaint relates to a member of staff, the matter must always be referred to the principal for action. Incidents involving the principal should be reported to the Head of School. Incidents involving the Head of School should be reported to the Managing Partner.

- The school's e-safety officer keeps a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.

- E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the designated child protection officer/DSP, who will make a decision as to whether or not to refer the matter to the police and/or Safeguarding and Social Care in conjunction with the head teacher.

Although it is intended that e-safety strategies and policies should reduce the risk to students whilst on-line, this cannot completely rule out the possibility that students may access unsuitable material on the internet. ICS cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

4.2 Unintentional access of inappropriate websites

- If a student or teacher accidentally opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately (and calmly) close or minimise the screen.

- Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.

- The incident should be reported to the e-safety contact officer and details of the website address and URL provided.

- The e-safety contact officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

- It is essential that teachers ensure that where they have an asked for filtering to be lifted for a particular lesson (eg: sex education) that they notify the Schools IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by students or staff.

4.3 Intentional access of inappropriate websites by a student

- If a student deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

- The incident should be reported to the e-safety officer and details of the website address and URL recorded.

- The e-safety officer should liaise with the network manager or Schools IT team to ensure that access to the site is blocked.

- The student's parents should be notified of the incident and what action will be taken.

4.4 Inappropriate use of ICT by staff

- If a member of staff witnesses misuse of ICT by a colleague, they should report this to the principals and the e-safety officer immediately.

- The e-safety officer should notify the network manager so that the computer or laptop is taken out of use and securely stored in order to preserve any evidence. A note of any action taken should be recorded on the e-safety incident report form.

- The e-safety officer should arrange with the network manager or Schools IT team to carry out an audit of use to establish which user is responsible and the details of materials accessed.

- Once the facts are established, the principal should take any necessary disciplinary action against the staff member and report the matter to the Head of School who will report to the Managing Partner and the police where appropriate.

- If the materials viewed are illegal in nature the Head of School should report the incident to the police and follow their advice, which should also be recorded on the e-safety incident report form.

4.5 Cyber bullying

4.5.1 Definition and description

Traditionally, bullying took place face to face in the physical world; online, bullying can take on a new dimension with technologies such as email, mobile phones and social networking sites used as a platform to hurt, humiliate, harass or threaten victims.

Cyber bullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim’s home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Cyber bullying is extremely prevalent as students who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text

- posting insulting, derogatory or defamatory statements on blogs or social networking sites

- setting up websites that specifically target the victim

- making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, “happy slapping”).

Cyber bullying can affect students and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, cyber bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

4.5.2 Dealing with incidents

The following covers all incidents of bullying that involve students at the school, whether or not they take place on school premises or outside school.

- ICS’ anti-bullying and behaviour policies and acceptable use policies cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of cyber bullying should be reported to the e-safety officer who will notify record the incident on the incident report form and ensure that the incident is dealt with in line with the school’s anti-bullying policy. Incidents should be monitored and the information used to inform the continuous development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone’s life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of e-safety awareness and education, students should be told of the “no tolerance” policy for cyber bullying and encouraged to report any incidents to their teacher.

- students should be taught:

    - to only give out mobile phone numbers and email addresses to people they trust
    - to only allow close friends whom they trust to have access to their social networking page
    - not to respond to offensive messages
    - to report the matter to their parents and teacher immediately.

- Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

4.5.3 Action by service providers

All website providers and mobile phone companies are aware of the issue of cyber bullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The student should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The student should also consider changing email address.

- Where bullying takes place in chat rooms, the student should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully’s access to the site can be blocked.

- Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

4.5.4 Cyber bullying of teachers

- The principals should be aware that teachers may become victims of cyber bullying by students. Because of the duty of care owed to staff, principals should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against students.

- Incidents of cyber bullying involving teachers should be recorded and monitored by the e-safety officer in the same manner as incidents involving students.

- Teachers should follow the guidance on safe ICT use in this policy and avoid using their own mobile phones or email addresses to contact parents or students so that no record of these details becomes available.

- Personal contact details for teachers should not be posted on the school website or in any other school publication.

- Teachers should follow the advice above on cyber bullying of students and not reply to messages but report the incident to the head teacher immediately.

4.6 Risk from inappropriate contacts

Teachers may be concerned about a student being at risk as a consequence of their contact with an adult they have met over the internet. The student may report inappropriate contacts or teachers may suspect that the student is being groomed or has arranged to meet with someone they have met online .

- All concerns around inappropriate contacts should be reported to the e-safety contact officer and the designated child protection officer/DSP.

- The designated child protection officer/DSP should discuss the matter with the referring teacher and where appropriate, speak to the student involved, before deciding whether or not to make a referral to Safeguarding and Social Care and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- Teachers should advise the student how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated child protection teacher and the e-safety officer should always notify the student’s parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child’s safety.

- Where inappropriate contacts have taken place using school ICT equipment or networks, the e-safety contact officer should make a note of all actions taken and contact the network manager or Schools IT team to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other students is minimised

4.7 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Staff need to be aware of those students who are being targeted by or exposed to harmful influences from violent extremists via the internet. students and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- ICS ensures that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism.

- All incidents should be dealt with as a breach of the acceptable use policies and the school’s behaviour and staff disciplinary procedures should be used as appropriate.

- The e-safety officer and the designated child protection officer/DSP should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.

5 SANCTIONS FOR MISUSE OF SCHOOL ICT

5.1 Sanctions for students

5.1.1 Category A infringements

These are basically low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions could include referral to the class teacher or tutor as well as a referral to the e-safety contact officer.

5.1.2 Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate, such as:

- continued use of non-educational sites during lessons
- continued unauthorised use of email or mobile phones
- continued use of prohibited sites for instant messaging or social networking
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions could include:

- referral to class teacher or tutor
- referral to e-safety contact officer
- loss of internet access for a period of time
- removal of mobile phone until the end of the day
- contacting parents.

5.1.3 Category C infringements

These are deliberate actions that either negatively affect the school IT system or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- cyber bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions could include:

- referral to class teacher or tutor
- referral to e-safety contact officer
- referral to principal
- loss of access to internet use for a period of time
- contact with parents
- any sanctions agreed under other school policies

5.1.4 Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme cyber bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions could include:

- referral to principal
- contact with parents
- possible exclusion
- removal of equipment
- referral to community police officer

5.2 Sanctions for staff

These should reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children.

5.2.1 Category A infringements

These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the principal.

- excessive use of internet for personal activities not connected to professional development
- any behaviour on the internet that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or students or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- breaching copyright or licence by installing unlicensed software.

Possible sanctions include referral to the principal who will issue a warning.

5.2.2 Category B infringements

These infringements involve deliberate actions that undermine safety on the school IT system and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Safeguarding and Social Care.

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Possible sanctions include:

- referral to the head teacher
- removal of equipment
- referral to police
- suspension pending investigation
- disciplinary action in line with school policies

Appendix 1:

Acceptable use policy for primary school students

Name:
School:
Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend
- only email people I know or if my teacher agrees
- only use my school email address
- talk to my teacher before using anything on the internet
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.

Parents

□ I have read the above school rules for responsible internet use and agree that my child may have access to IT services via the school IT systems. I understand that the school will take all reasonable precautions to ensure students do not have access to inappropriate websites, and that the school cannot be held responsible if students do access inappropriate websites.

□ I agree that my child's work can be published on the school website.

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:
Date:

Appendix 2:

Acceptable use policy for secondary school students

Name:
School:
Class:

I understand that all computer equipment is owned by the school and that I can use ICS IT systems as long as I behave in a responsible way that keeps me and others safe. I also understand that internet use at ICS is monitored and that if I do not follow the rules, I may not be allowed to use the school computers.

I will:

- only use the school's computers for school work and homework

- only delete my own files and not look at other people’s files without their permission

- keep my login and password safe and not let anyone else use it or use other people’s login or password

- not bring in files to school without permission

- ask a member of staff for permission before using the internet

- not visit websites I know are banned by the school

- only email people I know or whom my teacher has approved

- make sure any messages I send or information I upload is polite and sensible

- not open attachments or download files unless I have permission or I know and trust the person who sent it

- not give out my home address, phone numbers or send photographs or videos or give any other personal information that may identify me, my family or my friends unless my teacher has given permission

- never arrange to meet someone I have only met on-line unless my parent, carer or teacher has given me permission and I will take a responsible adult with me

- tell my teacher or responsible adult if I see anything I am unhappy with or receive a message I do not like and I will not respond to any bullying messages

- only use my mobile phone in school when I have permission and in the mobile device zones

- not use any internet system to send anonymous or bullying messages or to forward chain letters

- log out when I have finished using the computer.

Signed:
Date:

Parents

□ I have read the above school rules for responsible internet use and agree that my child may have access to ICS IT provision. I understand that the school will take all reasonable precautions to ensure students do not have access to inappropriate websites, and that the school cannot be held responsible if students do access inappropriate websites.

□ I agree that my child’s work can be published on the school website.

□ I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:
Date:

Appendix 3

Acceptable use policy for staff

Access and professional use

- All computer networks and systems belong to the school and are made available to staff for educational, professional and administrative purposes only.

- Staff are expected to abide by all school e-safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken.

- The school reserves the right to monitor internet activity and examine and delete files from the school’s system.

- Staff have a responsibility to safeguard students in their use of the internet and reporting all e-safety concerns to the e-safety contact officer.

- Copyright and intellectual property rights in relation to materials used from the internet must be respected.

- E-mails and other written communications must be carefully written and polite in tone and nature.

- Anonymous messages and the forwarding of chain letters are not permitted.

- Staff should not access inappropriate websites or chat rooms.

Data protection and system security

- Staff should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.

- Use of any portable media such as USB sticks or DVD-ROMS is not allowed unless permission has been given by the network manager and a virus check has been carried out.

- Downloading executable files or unapproved system utilities are blocked and cannot be installed.

- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

- Files should be saved, stored and deleted in line with the school policy.

Personal use

- Staff should not browse, download or send material that could be considered offensive to colleagues and students or is illegal.

- Staff should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.

- Staff should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

- ICS IT systems should not be used for personal financial gain, gambling, political purposes or advertising.

I have read the above policy and agree to abide by its terms.

Name:
School:
Signed:
Date:

Appendix 4:

E-safety incident report form

School/organisation's details:

Name of school/organisation:

Address:

Name of e-safety contact officer:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (cyber bullying
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Description of incident

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ cyber bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ e-safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to head teacher/senior manager
□ advice sought from Safeguarding and Social Care
□ referral made to Safeguarding and Social Care
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ e-safety policy to be reviewed/amended

Outcome of incident/investigation

Appendix 5

STUDENT CODE OF CONDUCT FOR NETBOOKS LOAN CHARTER

Our students will be expected to use the netbook allocated to them appropriately following the conduct outlined in the Netbook Loan Charter.

Student name and surname: ____________________

Parent/Guardian name and surname: ____________________

Purpose

The school ICT initiative "Using Netbooks for e-learning" aims to improve student learning experiences both in and out of the classroom. The students may use the Netbook for a particular topic of work, school projects or need.

Ownership

The loaned Netbooks remain school property and ownership is not transferable to students. If the loaned Netbook gets damaged or lost, the student will be required to replace the Netbook.

Please note: a Netbook Loan Charter must be provided to the students and signed before the Netbook will be loaned.

Students and parents/guardians must carefully read this charter prior to signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

Netbook Loan Charter

I have read the Netbook Loan Charter.

I understand my responsibilities regarding the use of the Netbook and the Internet.

In signing below, I acknowledge that I understand and agree to the Netbook Loan Charter.

I understand that failure to comply with the Netbook Loan Charter could result in loss of future loan permission.

Signature of student: ___________________________ Date: / /

Signature of parent/guardian: ___________________________ Date: / /

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

For Office use only
Netbook User Account No: _____________________
Netbook Registration No: _____________________

LOAN CHARTER

1. Purpose

The digital Netbook is to be LOANED as a tool to assist student learning both at school and at home.

2. Equipment

2.1 Ownership

2.1.1 The student must bring the Netbook fully charged to school every day if required. Chargers should be left at home.

2.1.2 The school retains ownership of the Netbook.

2.1.3 All material on the Netbook is subject to review by school staff. If there is a police request, ICS will provide access to the Netbook and personal network holdings associated with your use of the Netbook.

2.2 Damage or loss of equipment

2.2.1 All Netbooks and batteries are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the Netbook. It does not cover negligence, abuse or malicious damage.

2.2.2 Any problems, vandalism, damage, loss or theft of the Netbook must be reported immediately to the school.

2.2.3 In the case of suspected theft, a police report must be made by the family and an event number provided to the school.

2.2.4 In the case of loss or accidental damage, a parent/guardian should write and sign a statement about how it happened.

2.2.5 Netbooks that are damaged or lost by neglect, abuse or malicious act, may need to be paid for. The Director of ICT will determine whether replacement is appropriate and/or whether or not the student is responsible for repair or replacement costs and whether or not the student retains access to Netbook loans.

2.2.6 Students will be required to replace lost or damaged chargers.

3. Standards for digital Netbook care

The student is responsible for:

i) Taking care of Netbooks in accordance with school guidelines.

ii) Backing up all data securely. This should be on a memory stick, online storage or on other external storage device. Students must be aware that the contents of the Netbooks may be deleted and the storage media reformatted in the course of repairs.

iii) Never damaging or disabling digital Netbooks, Netbook systems and networks or establishing, participating in or circulating content that attempts to undermine or bypass Netbook security mechanisms for either software or hardware.

4. Acceptable computer and Internet use

Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

4.1 Access and Security

4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their computer or network account.
- log off at the end of each session to ensure that nobody else can use their computer or network account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Immediately report to supervising adult (teacher/parent/guardian) if another online user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:
    - a message that was sent to them in confidence
    - a computer virus or attachment that is capable of damaging recipients' computers
    - chain letters and hoax emails
    - spam, e.g. unsolicited advertising material.
- never send or publish:
    - unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
    - threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
    - sexually explicit or sexually suggestive material or correspondence.
    - false or defamatory information about a person or organisation.
- ensure that personal use is kept to a minimum and Internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
- never damage or disable computers, computer systems or networks of ICS.

- ensure that services are not used for unauthorised commercial activities, online gambling or any unlawful purpose.
- be aware that all use of Internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.2.1 Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

4.3.1 Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the Internet or Intranet has the approval of their teacher and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1 Students will be aware that:

- they are held responsible for their actions while using Internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access Internet and online communication services.
- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

5.1.1 any Internet site accessed that is considered inappropriate.

5.1.2 any suspected technical security breach involving users from other schools or other organisations.

Updated: January 2014
Review Date: January 2015
Appendix 6

ICS NETBOOK

LOAN

CHARTER

FOR STUDENTS

We are excited about the introduction of NETBOOKS as valuable digital tool for learning. The students will be expected to use netbooks appropriately following the conduct provided in the Netbook Loan Charter.

Student name and surname: ----------------

Parent/Guardian name and surname: ------------

Purpose

The school ICT initiative "a Netbook For Every Student" aims to improve student learning experiences both in and out of the classroom. The students may use the netbook for a particular topic of work , school project or need.

Ownership

The loaned netbooks remain school property and ownership is not transferable to students. If the loaned netbooks gets damaged or lost, the student will be required to replace the netbook .

Please note: a Netbook Loan Charter must be provided to the students and signed before the netbook will be loaned.

Students and parents/guardians must carefully read this charter prior signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

Netbook Loan Charter

I have read the Netbook Loan Charter.

I understand my responsibilities regarding the use of the digital netbook and the Internet. In signing below, I acknowledge that I understand and agree to the Netbook Loan Charter.

I understand that failure to comply with the Netbook Loan Charter could result in loss of future loan permission.

Signature of the student: _ date: / /

Signature of the Parent/Guardian: date : / /

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

Office user Account No: --------------

Netbook Registration No_________________

ICS Netbook Loan Charter

1. **Purpose**
   The digital netbook is to be LOANED as a tool to assist student learning both at school and at home.

2. **Equipment**
   2.1 Ownership
   2.1.1 The student must bring the netbook fully charged to school every day if required. Chargers should be left at home.

   2.1.2 The school retains ownership of the netbook.

   2.1.3 All material on the netbook is subject to review by school staff. If there is a police request, ICS will provide access to the netbook and personal network holding associated with your use of the netbook.

2.2 Damage or loss of equipment
2.2.1 All netbooks and batteries are covered by a manufacturer's warranty. The warranty covers manufacturer's defects and normal use of the netbook. It does not cover negligence, abuse or malicious damage.

2.2.2 Any problems, vandalism, damage, loss or theft of the netbook must be reported immediately to the school.

2.2.3 In case of suspected theft a police report must be made by the family and an event number provided to the school.

2.2.4 In case of loss or accidental damage a witnessed statutory declaration signed by a parent should be provided.

2.2.5 Netbooks that are damaged or lost by neglect, abuse or malicious act, may require reimbursement. The Director of ICT will determine whether replacement costs and whether or not the student is responsible for repair or replacement costs and whether or not the student retains access to netbook loans.

2.2.6 Students will be required to replace lost or damaged chargers.

2.2.7 ICS does not provide hardware repair assistance. It is fine for ICS to have the netbook repaired at your own expense. If the netbook is returned in working order, ICS has no reason to charge for damages. Any replacement must be as the original was. ICS will not accept any differences.

2.2.8 The liability is not related to the place where the damage may occur. Students remain responsible of the loaned item(s).

3. **Standards for digital netbook care**

The student is responsible for:

i) Taking care of netbooks in accordance with school guidelines.

ii) Backing up all data securely. This should be on a memory stick, online storage or on other external storage device. Students must be aware that the contents of the netbooks may be deleted and the storage media reformatted in the course of repairs.

iii) Never damaging or disabling digital netbooks, netbook systems and networks or establishing, participating in or circulating content that attempts to undermine or bypass netbook security mechanisms for either software or hardware.

4. Acceptable computer and Internet use

Students are not to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

4.1 Access and Security

4.1.1 Students will:

- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
- ensure that communication through Internet and online communication services is related to learning.
- keep passwords confidential, and change them when prompted, or when known by another user.
- use passwords that are not obvious or easily guessed.
- never allow others to use their computer or network account.
- log off at the end of each session to ensure that nobody else can use their computer or network account.
- promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
- Immediately report to supervising adult (teacher/parent/guardian) if another online user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
- never knowingly initiate or forward emails or other messages containing:

  a a message that was sent to them in confidence.

  a a computer virus or attachment that is capable of damaging recipients' computers.

  a chain letters and hoax emails.

  a spam, e.g. unsolicited advertising material.

- never send or publish:

  a unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.

  a threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.

  a sexually explicit or sexually suggestive material or correspondence.

  o false or defamatory information about a person or organisation.

- ensure that personal use is kept to a minimum and Internet and online communication services are generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.

- never damage or disable computers, computer systems or networks of ICS.
- ensure that services are not used for unauthorised commercial activities, online gambling or any unlawful purpose.

- be aware that all use of Internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.2.1 Students will:

- never publish or disclose the email address of a staff member or student without that person's explicit permission.
- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

4.3.1 Students will:

- never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
- ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
- ensure any material published on the Internet or Intranet has the approval of their teacher and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1 Students will be aware that:

- they are held responsible for their actions while using Internet and online communication services.
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access Internet and online communication services.

- the misuse of Internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1 Students will report:

5.1.1 any Internet site accessed that is considered inappropriate.

5.1.2 any suspected technical security breach involving users from other schools or other organisations.