Hornsea School & Language College

ICT and E-Safety Policy

Created by:	John Hart	
Date Created:	December 2009 – Merged with ICT Policy November 2012	
Approved by:	**Headteacher:** 06.12.17	**Governing Body:** 06.12.17
Last Reviewed:	**Date:** November 2017	**By:** John Hart & Damian Brocklehurst
Date of Next Review:	November 2018	

ICT and E-Safety Policy

Introduction

This document is a statement of the aims, principles, strategies and procedures for the use of Information and Communications Technology both in the ICT department and throughout the school. It also recognizes the risks involved in technology and therefore encompasses the E-Safety Policy.

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Cyber Bullying, Curriculum, Data Protection and Security.

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of content filtering.
- National Education Network standards and specifications.

Contents

Policy

Appendices

Information and Communication Technology

The distinctive contribution of information and communication technology to the school curriculum.

Information and communication technology (ICT) contributes to the school curriculum by preparing all children to participate in a rapidly changing society in which work and other forms of activity are increasingly dependent on ICT. The subject develops pupils' information skills, including the ability to use information sources and ICT tools to help them find, explore, develop, analyse, exchange and present information and to support their problem solving, investigative and expressive work. An essential part of ICT capability is evaluating information and the ways in which it may be used, and making informed judgements about when and how technology can be used. Pupils also develop understanding of the implications of ICT for working life and society. The use of ICT significantly enhances teaching and learning in other subjects by enabling rapid access to knowledge, information and experiences from a wide range of sources. The use of ICT throughout the curriculum encourages critical thinking, imagination and creativity, problem solving, initiative and independence, teamwork and reflection.
The addition of Computing to the curriculum allows pupils the opportunity to create digital technology and software for themselves and gives them an understanding of how the systems that they use work; therefore making students better informed and more responsible users.

Aims

Through the use and teaching of ICT/ Computing the school aims to:

- Meet the requirements of Curriculum 2014, enhancing Digital literacy
- Help other curriculum areas meet the requirements of curriculum change through the support of ICT
- Allow staff and children to gain confidence in, and enjoyment from, the use of ICT and Computing
- Allow children to develop specific ICT and Computing skills as set down in the school's scheme of work allowing them to evaluate which of these routes would suit further study at KS4 and KS5.
- Ensure that staff and children alike understand the capabilities and limitations of ICT and gain insight into the implications of its development for society
- Allow teaching staff to develop professionally by enhancing their teaching skills, management skills and administrative skills
- Support all trainee teachers in their use of ICT in the curriculum as part of their Initial Teacher Training in accordance with **'**Qualifying to Teach: Professional Standards for Qualified Teacher Status and Requirements for Initial Teacher Training' DfES, 2002

Care of Classroom Equipment

The individual in whose care it is trusted should maintain all ICT equipment in a clean and serviceable state.

- All users should log off at the end of each session

- Any technical fault should be reported immediately via the technical forum accessible via the staff area of the school website, pupils should not be permitted to solve issues with hardware.

- The use of solvent cleaners and polishes is not allowed without express permission from the Network Managers.

- ICT areas should be left as staff would like to find them with mice and keyboards replaced appropriately

Care of Loaned Equipment

- Equipment may be in the care of a specific individual, but it is expected that all staff and pupils may wish to benefit from the use of an IPad, laptop computer or other ICT equipment and access should be negotiated with the individual concerned. Pupils must sign in to all borrowed ICT equipment with their network username and password and are not permitted to share accounts.

- Certain equipment (e.g. digital camera) will remain in the ICT resource area, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the resource area; such equipment should be signed in and out so a clear record is kept of who has responsibility for loaned equipment.

- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy.

- Equipment used in conjunction with a school-approved excursion does not require the signing of such a disclaimer.

- Any costs generated by the user at home, such as phone bills etc. are the responsibility of the user.

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.

Role of the ICT Faculty and Leadership Link

The responsibilities include:

- Contributing to the ICT and E-Safety Policy

- Maintenance of a Scheme of Work that reflects current resources, National Curriculum, staff and child skills etc.

- Monitoring of implementation of the Scheme of Work in ICT department including issues such as equality of access, planning and assessment etc.

- To provide support in the delivery of the school's Scheme of Work through monitoring, advice, provision of sample lessons and activities etc. according to the needs of the individual member of staff. This will include reporting to the Headteacher when appropriate.

- To monitor new developments in ICT (through the attendance of appropriate INSET) and integrate these into action plans, schemes of work and policies where appropriate.

- To liaise with the relevant individuals, especially in the area of network maintenance to ensure that the integrity of the system is not threatened in the event of illness, staff departure etc.

Planning, Recording, Assessment and Monitoring In ICT Lessons.

ICT opportunities should be identified in all schemes of learning and show the contribution that each area is making to the development of ICT knowledge understanding and skills.

All children will be assessed on entry to y7 for their current ICT attainment band according to Pixel band descriptors defined by our centre. This assessment is in the form of self-evaluation where the user documents their competencies against a diagnostic matrix. The results of this assessment and teacher judgement will determine a working level for ICT. A follow up assessment will also take place each term. In years 9 to 11 work is assessed against appropriate examination standards and students are given feedback on how to achieve a pass or move to the next level so that they are appropriately prepared for examination entry. This assessment data will be shared in the annual report. A summary report will also be presented to the Governors annually.

E-safety at Hornsea School

The school will appoint an e-Safety group. This will be the Designated Child Protection Officer (Mr Chris Hamling), a member of the SLT (Mr R Lewchenko) and the E-Learning Co-ordinator (Mr J Hart).

Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and will be approved by Governors.

The e-Safety Policy will be reviewed annually.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient (online teaching and learning resources, facilitating 24:7 'anywhere' access)
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;

- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- The school will maintain a current record of all staff and students who are granted Internet access
- Parents will be informed that students Internet access will be monitored and that it is not possible to filter all unsuitable sites
- Parents will be asked to sign and return a consent form for student access
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement
- All pupils have access to the guest wifi. Y11-13 have access to it during lesson time to allow them to use their own devices for research, for example during study periods. Y7-10 have access outside of lesson times. Filtering varies by year group and is age appropriate

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the Network Managers (Mr Rob Coles & Miss Faye Dickinson) via helpdesk @hslc.co.uk
- Teachers should ensure that the use of Internet derived materials by students and staff complies with copyright law
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- Staff should ensure that any videos shown from the internet are age appropriate and check the content of any links they will access in lessons.

Email

- Students may only use approved e-mail accounts on the school system
- Students must immediately tell a teacher if they receive offensive e-mail and this should be reported to the E-safety Coordinator (HJJ)
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Staff should not disclose any personal details about themselves when communication via email to students.

- All communication with students should be through the school email system (i.e. @hslc.co.uk) and not through staff members or pupils' personal email accounts. Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- Where possible staff should use Edulink to ensure email is targeted at appropriate staff rather than using the "allstaff" or "teachingstaff" addresses. This will reduce the amount of time wasted by reading emails that are not applicable to the receiver.

Social Networking

- The School will block/filter access to social networking sites and newsgroups unless a specific use is approved by the head
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Twitter Policy

Twitter is increasingly being used by departments as a valuable link between the school, parents and pupils. Departments should follow the following policy when setting up and administering accounts.

- School twitter accounts need to be approved by the head.
- The username and password must be shared with the e-safety coordinator.
- If you are approved to represent the school, unless you are specifically authorised to speak on behalf of the school as a spokesperson, you should state that the views expressed in your postings, etc. are your own. Stick with discussing school-related matters that are within your area of responsibility.
- Tweets must never be derogatory to any person or bring the school name into disrepute. Remember Twitter is a public platform
- You must never engage by direct message with a pupil.
- You will retain a personal/professional boundary at all times.
- You will check for photo permissions for any images of pupils posted. The pupils should not be able to be matched to a name in your text. First names only should be used when referencing pupils
- The school Twitter account will only follow educationally linked accounts. No personal accounts, including pupils will be followed.
- The school Twitter account will not reply to any 'replies' on Twitter. This is not the platform to discuss or debate school related issues.

Filtering

Hornsea School will be using a professional, versatile proxy server that filters Web content using a number of techniques. These include real-time context analysis in multiple languages, a known database of categorised sites and sophisticated image content analysis.

Hornsea School uses SSL Intercept Mode. This is a means every time you visit a site in the form https://somesite.com the Smoothwall software will decrypt, check and re-encrypt the traffic before continuing communication with the target site. Sites excluded include banking etc.

As students progress through school they are given greater responsibility as the filtering of internet use is reduced. 6th Formers for example have access to YouTube to allow them to access its many

educational resources They receive a letter to highlight the responsibility of this degree of filtering and are aware that this privilege could be removed if abused.

Computer monitoring

- Impero network management software is used to monitor network users activities at all time. Key word libraries are used to safeguard users by capturing on screen activity and time stamping violations

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a video conference call
- Videoconferencing will be appropriately supervised for the pupils' age

Managing Emerging Technologies including Tablet Computers & Mobile Telephones

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones will not be used for personal use during lessons or formal school time (student's mobile phones should normally be switched off and out of sight during lesson time). However, the teacher in charge may give permission for the use of mobile phones for educational purposes, e.g Filming, recording and in some subjects for listening to music whilst working.
- The sending of abusive or inappropriate text messages is forbidden
- Edulinkone the chosen method of SMS contact with parents and students

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The management team will ensure that content is accurate and appropriate

Publishing Students' Images and Work

- Photography and Video: Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is published for any purpose. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet.
- Photographs that include students will be selected carefully and will be appropriate for the context
- Students' full names will not be used anywhere on the Web site or social media, particularly in association with photographs
- Permission from parents or carers will be obtained before photographs or video of students are published on the school web site or social media
- Work can only be published with the permission of the student and parents. The E-learning co-ordinator will keep a list of those parents objecting and this is accessible by all staff in the Sims database

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly

- Security strategies will be reviewed by the ICT Department.
- Laptops (supplied by the school for teachers) should be connected to the school network at least once per calendar month to allow for anti-virus scans / updates to occur and software updates to be installed
- Access to USB memory sticks is disabled as the data on them is not encrypted.

Internet Danger Awareness

All teaching staff and all pupils will be made aware of the potential dangers of online activity and trained in Internet safety under the ThinkUKnow scheme by CEOP as a minimum. Annual online e-safety training is also completed by teaching staff

A program of E-safety education will be delivered throughout the year by the e-safety co-ordinator. It covers Cyberbullying for y8, sexting for y9, using ICT in the workplace in y10 and digital footprints in y11. These messages are supplemented and reinforced by assemblies.

Year 7 pupils follow the BCS Esafety Training programme in ICT Lessons.

Parents are also alerted to topical issues relating to internet danger by emails and newsletters from the e-safety co-ordinator. Online training is also offered to all parents.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor East Riding of Yorkshire Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Access to inappropriate images and Internet usage

There are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to Hornsea School to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. School equipment can be monitored to guard against inappropriate usage.

Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Organisations and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the CP Officer should be immediately informed (depending on material / circumstances the police and Local Authority

Designated Officer (LADO) may also be informed). Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the Network Managers, Head of ICT or E-learning co-ordinator
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure

Communication of Policy

Students

- Rules for Internet access will be posted in all ICT suites
- Students will be informed that Internet use will be monitored
- Advice and e-safety information available to students via Hornsea School Website .

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic will be monitored and 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.

Parents

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Web site
- Advice and e-safety information available to parents via Hornsea School website (under "E-Safety" link)
- Parents should be aware that the school will take any reasonable action to ensure the safety of its students: in cases where the school has reason to be concerned that any child may be subject to ill-treatment, neglect or any other form of abuse, the school has no alternative but to follow the Hornsea School Child Protection Policy and inform Children's Services of their concern.

Visitors

- Visitors / guests to Hornsea School must abide by e-safety procedures and policies as set out in this booklet. It is the responsibility of the supervising staff member to make them aware of possible policy violations. Longer term access can be arranged with network accounts subject to clearance with Human Resources.

Staff should also refer to the Guidance for School Safe Working Policy and Staff Acceptable Use Policy for further information.

Appendices

Referral Process – Appendix A

E-Safety Rules– Appendix B

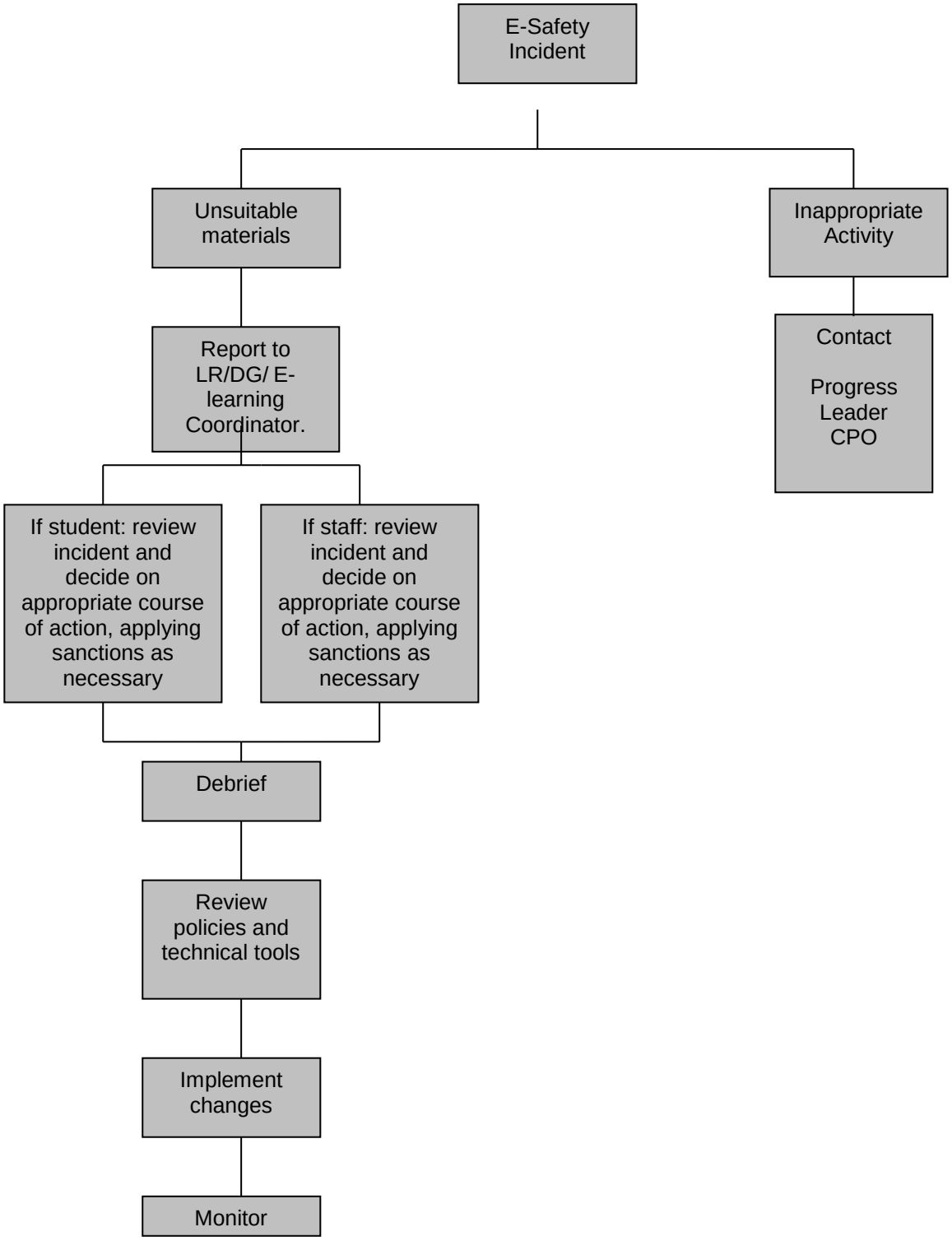
Letter to parents – Appendix C

E-Safety Audit – Appendix D

HSLC ICT Sanctions – Appendix E

Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta – E-safety 2005

Appendix B

E-Safety Rules (for learners)

These e-Safety Rules help to protect students and the school by describing acceptable and unacceptable computer and mobile phone use.

- The school owns the computer network and can set rules for its use.
- It may be a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- When communicating with staff, I should always use my school email account
- Social networking sites such as Facebook are not to be accessed in school
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers. This includes text messages sent from mobile phones. Users should consider the feelings of others and not post hurtful or damaging images or text
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing any media considered to be unauthorised or unlawful including text, imagery or sound.

Appendix C

Hornsea School & Language College

E-Safety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the Curriculum. Both students and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Student Name:	**Form:**

Students' Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network, Internet access and email use may be monitored.

Signed:	**Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published on the school website or on social media, subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**

Please print name:

Please complete, sign and return to the school

Appendix D

E-Safety Audit – Secondary Schools

This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	Y/N
Date of latest update: 24th November 2017	
The Policy was agreed by governors on:	
The Policy is available for staff at: Hornsea School Website Staff Area ("Internet Safety" link)	
And for parents at: Hornsea School Website (under "Internet Safety" link)	
The designated Child Protection Teacher/Officer is: Mr Chris Hamling	
The E-Learning Coordinator is: Mr J. Hart	
Has e-safety training been provided for both students and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix E

HSLC ICT SANCTIONS

Minor offence (silly unblock requests, copyright infringement, small numbers of mp3s, wasteful printing, silly pictures)	Temporary disabling of the account until reprimand is given
Internet offences, e.g use of proxy sites and inappropriate websites.	1 week in walled garden Incident slip completed and Performance managers notified
Second offence	2 weeks in walled garden Incident slip completed and Performance managers notified
Third offence	4 weeks in walled garden Incident slip completed and Performance managers notified
Serious offence (pornography, cyber bullying, using another pupil's password or 4th minor offence)	Detention with Leadership Team Incident slip completed and Performance managers notified
Pupils will remain in walled garden until they have returned their signed Internet Safety Agreement form. **All offences will be recorded in Sims**	