THE CHORISTER SCHOOL
DURHAM CATHEDRAL

ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY INCLUDING INTERNET, MOBILE PHONES AND INTERNET ENABLED SMART WATCHES

Policy on website

January 2019

1. Introduction

The Chorister School is committed to upholding the principles and values set down in the Keeping Children Safe in Education (2018). All teaching and administrative staff undertake the Prevent Awareness training on an annual basis (January 2019 last completed), and are aware of the risks posed by the threat of radicalisation and extremists using social media. An effective approach to online safety empowers the school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

Online safety can be considered to be categorized into three areas of risk:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subject to harmful online interaction with other users

Conduct – personal online behavior that increases the likelihood of, or causes, harm

Technology plays a significant part in the process of teaching and learning at The Chorister School. It is a crucial component of every academic subject, and is also taught as a subject in its own right. Most of our classrooms are equipped with interactive whiteboards, projectors and computers. We have an ICT suite and iPads in the school and pupils may use the machines, under the supervision of a member of staff.

Pupils are taught how to research using the internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution. Some sites that appear to be legitimate, impartial, historical sites, actually masquerade as sources of racist, homophobic, jihadist or other propaganda. Some free, on-line encyclopedias do not evaluate or screen the material posted on them.

The School Network enables pupils to access the system's resources from any of the classrooms. This access, including use of the Internet, raises a large number of legal, technical and ethical issues. Proper regulation of staff and pupil use of resources is covered in this policy. All those who wish to make use of the available resources must comply with this policy.

The Chorister School is committed to the safe and responsible use of the internet as schools have a vital role to play in protecting pupils from the extremism and radicalisation. The Chorister School keeps children safe from the risks of terrorist exploitation on social media in the same way it approaches safeguarding children from any other online abuse. The Chorister School works closely with its network provider in order to ensure that the filtering and blocking of websites is of the highest standard so the risk of inappropriate material is minimised.

Limitation in the provision of hardware and the vigilance of teachers and parents have a part to play in the safeguarding and protection of pupils at school and children at home.

2. The Policy Document

This document must be read and understood by all Staff and Pupils wishing to use the School Network and by parents wishing their children to bring mobile phones or internet enabled smart watches to school. Copies of the document are available in the ICT suite, the School Website and the school lists area on the server. Strict adherence to the policy is required by all users.

Internet enabled smart watches, with a separate data contract and the ability to access the internet without being linked to wifi network or a smart phone, should be handed into reception during the school day, in the same way as mobile phones are. The Bluetooth function of any internet enabled smart watch should be turned off at all times in school so that communication with others via messaging or the sending of pictures is impossible.

Sanctions

Any deviation from the Policy will result in a temporary or permanent ban on the use of the School Network or of the Internet.

Further action may be taken in line with the existing School practice on inappropriate language or behaviour.

When necessary, the School may be under a legal requirement to contact the Police or other authorities as required by our Safeguarding Policy. (See Misuse: Statement of Policy below)

The Role of Technology in Our Pupils’ Lives

Technology plays an important part in the lives of all young people. Sophisticated games consoles, or PSPs (play stations portable), like Wiis and Nintendo DS, together with Bluetooth mobile phones and internet enabled watches provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter and Tumblr), to skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms and social networking sites (such as Instagram and Facebook) and video sharing sites (such as YouTube).

The communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at The Chorister School to teach pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation. Pupils also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment. Pupils will be educated about e-safety issues and appropriate behaviours so that they remain safe and legal online. We want pupils to develop critical thinking skills to reflect and enable them to keep themselves safe.

Role of Our Staff

With the explosion in technology, we recognise the inadequacies of blocking and barring sites. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves – this we feel we can best do by having a whole-school approach to on-line safety and ensuring a clear policy on the use of mobile technology. This message is reinforced by our Designated Safeguarding Leads and our teaching staff. The Bursar and our technical support providers have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT. They monitor the use of the internet and will report inappropriate usage to the teaching staff.

Role of our Child Protection Officers

We recognise that internet safety is a child protection and general safeguarding issue. Mr Wicks, Mrs Faulkner-Walford and Mr Chandler, our Designated Safeguarding Leads (DSL) have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. They work closely with the Local Safeguarding Children's Board (LSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of The Chorister School. All staff have pastoral responsibilities and have received training in e-safety issues. The school's comprehensive programme on e-safety is the responsibility of the ICT teaching staff. They will ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online. It is their responsibility to handle allegations of misuse of the internet within school.

Misuse: Statement of Policy

We will not tolerate any illegal material, and will always report illegal activity to the police and/or the Local Safeguarding Children Board (LSCB). If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy.

Involvement with Parents and Guardians

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact parents/guardians if we have any worries about your son or daughter's behaviour in this area, and we encourage parents/guardians to share any worries with us. We recognise that not all parents/guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. Parents of pupils in Forms 4, 5 and 6 are invited to attend a Parent Awareness meeting which provide them with information on e-safety and showed the measures in place to guide our pupils so that they remain safe and legal online.

In addition to this, parents and guardians are required to sign an Acceptable Use of the Internet Form (AUF) and discuss the requirements and responsibilities of their child when using the internet at the Chorister School, see Appendix A to this Policy. Appendix B should be completed and signed by the pupil. These forms will be sent out electronically each academic year and are required to be completed to enable children to access the internet at The Chorister School.

Pupils should not have any reason to have mobile phones or internet enabled smart watches (which are connected to the internet or have a data contract) with them during the school day. If a parent/guardian wishes their child to bring a phone or internet enabled smart watch to school parents/guardians must read, sign and return the 'Acceptable Use of Mobile Phones/Internet enabled smart watches Policy' see Appendix C.

Charter For The Safe Use Of The Internet and Electronic Devices at The Chorister School

"Children and young people need to be empowered to keep themselves safe. This isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim." Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

E-safety is a whole school responsibility. At The Chorister School, the staff and pupils have adopted the following charter for the safe use of the internet inside the school:

Cyberbullying

Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying, including peer on peer abuse, and cyberbullying.

Proper supervision of pupils plays an important part in creating a safe ICT environment at school; but everyone needs to learn how to stay safe outside the school.

We value all of our pupils equally. It is part of the ethos of The Chorister School to promote considerate behaviour, and to value diversity.

Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Staff are aware that pupils with SEN have an increased vulnerability to risk online, especially those with language and communication difficulties. For all pupils, including those with SEN, access to computers and the internet is always supervised and training is given on internet safety.

Inclusion and Equal Opportunities

We believe that all children have the right to access ICT and computing. In order to ensure that children with special educational needs achieve to the best of their ability, it may be necessary to adapt the delivery of curriculum for some pupils. We teach ICT and computing to all children, whatever their ability. Through the teaching of ICT and computing we provide learning opportunities that enable all pupils to make progress. We do this by setting suitable learning challenges and responding to each child's different needs. Where appropriate ICT and computing can be used to support SEN children on a one to one basis where children receive additional support.
Using ICT can:

- Address children's individual needs
- Increase access to the curriculum
- Enhance language skills

Our school promotes equal opportunities for computer usage. All pupils regardless of social class, gender, culture, race, ability or learning needs are to be provided with equal access to ICT facilities and teaching. All individuals will be given the opportunity to experience success in learning and to achieve their fullest potential through appropriately challenging tasks and computer resources. We celebrate the diversity in our school and in the world around us, as well as reinforcing fundamental British values through ICT and Computing. We are committed to ensuring our children respect themselves and others and can distinguish right from wrong whilst communicating online and face to face.

Treating Other Users with Respect

We expect pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face to face contact. We expect a degree of formality in communications between staff and pupils, and staff are not permitted to share their mobile phone number or private email address with pupils or to communicate with pupils on Facebook or other social networking sites. Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated, please refer to our Anti-bullying policy. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation, physical disability or special educational needs.

All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issue to a member of the pastoral staff.

All phones and internet enabled smart watches of day pupils that are brought into school are kept by the school reception staff and collected when children depart from school. The Boarding House have separate arrangements regarding the storage of mobile phones and internet enabled smart watches.

Keeping the School Network Safe

We have implemented a secure network and broadband in school, using internet filters, information system security and virus protection. The firewall was upgraded in October 2016 We have strong anti-virus protection on our network, which is operated by our IT provider, Total Business. Any member of staff or pupil, who wishes to connect a removable device to the school's network, is asked to arrange in advance with the IT provider to check it for viruses.

We use passwords to access devices, the internet and networks. We adhere to the BECTA guidelines regarding E-teaching and the internet. Certain sites are blocked by our filtering system and our IT provider monitors pupils' use of the network.

The IT provider monitors email traffic and blocks SPAM and certain attachments.

Access is via personal LOGIN, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.

Access to sites such as "hotmail" is not allowed on the school's network. (Except for supervised access for Boarders during non-school hours to maintain contact with their families).

Promoting Safe Use of Technology

Parents and pupils of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- Childnet International (www.childnet-int.org)
- Digizen (www.digizen.org.uk)
- E-Victims (www.e-victims.org)

- Bullying UK (www.bullying.co.uk)
- Thinkuknow (https://www.thinkuknow.co.uk/parents
- Be Internet Legends (https://beinternetlegends.withgoogle.com/en_uk)
- UK Safer Internet Centre (https://www.saferinternet.org.uk/)
- Parentzone (https://www.saferinternet.org.uk/)
- Educate against hate (https://educateagainsthate.com/)
- Net-aware (https://www.net-aware.org.uk/)
- Internet matters (https:www.internetmatters.org)

These sites prepare their own models of good practice, which form the subject of presentations at Assemblies and discussion in the meetings of the School Council. They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment, explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

Safe Use of Personal Electronic Equipment

Our guidance is that no one should put anything onto the web which they know to be unacceptable with the School's code of conduct. We teach pupils to have respect for others. We offer guidance on the safe use of social networking sites and cyberbullying in PSHCE lessons, which covers blocking and removing contacts from "buddy lists".

Our ICT lessons on e-safety include guidance on how pupils can identify the signs of a cyber-stalker, and what they should do if they are worried about being harassed or stalked online. We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.

Considerate Use of Electronic Equipment

Mobile phones, internet enabled smart watches and all other personal electronic devices should be named, switched off and stored securely at Reception during the school day.

Staff may confiscate personal equipment that is being used during the school day. This would usually be returned to the pupil's parent(s) at the end of the school day.

Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

We expect all pupils to adhere to this charter for the safe use of the internet. Copies are given to all pupils and their parents, and we may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones, smart phones, smart watches (internet enabled) and other electronic devices.

All Users

Access to the Network is provided to carry out school work, providing you agree to follow the rules as laid out below.

General school rules apply as much in the ICT Suite as in any part of the school.

Eating and drinking are prohibited near any computer, including iPads.

Applications and utilities are available to all users, although access to certain resources (ie

Internet) may be removed from certain users if considered necessary.

Desktop appearance and display properties are mandatory and cannot be changed. (ie Pupils

are unable to add shortcuts or change their settings)

The ICT Co-ordinator should be informed immediately of any Virus notification.

All Internet sites visited and software used is monitored.

Computer Access

Staff are responsible for turning off the computers in their teaching and office areas at the end of each school day.

Duty staff are responsible for switching off the computers in the ICT Suite at the end of each day.

Any computer, and the ICT Suite itself, should be left as someone would wish to find it.

ICT equipment should not be taken off site without permission from the Head of ICT.

Staff should supervise the use of the network as closely as possible during timetabled lessons. Pupils may only use the computers in the ICT Suite if a member of staff is present.

iPad Access

iPads must be signed in and signed out if they leave the ICT Suite on the form located in the ICT Suite.

iPads should not be taken off site without permission from the Head of ICT.

Anyone who misuses or does not look after the iPads will not be allowed to use them.

Security

All passwords are recorded by Total Business.

All users must log on with their own user name and password. They should not release their password to anyone except the ICT Co-ordinator.

Pupils must not access other users’ folders, work or files.

Users must not expect that their work or emails can be private. Pupils should understand that in the event of a police enquiry all user history may be traced, even those things which have been deleted.

Always log-off from a computer when you leave it, even for a few minutes.

Each user has a personal folder on the server on which to store their work. This can be accessed from any computer linked to the network.

All storage areas on the network are treated as school property.

The ICT Co-ordinator can view a computer screen at any time without the users' knowledge to ensure the system is being used properly.

Internet use is monitored by the system used in the school. This monitoring is controlled by the system administrator so that pupil access can be checked for misuse.

A log of all emails is recorded by the system. This consists of a record of sender, recipient, date and subject line.

A copy of every email sent by and to a pupil is sent to the system administrator. This is to ensure correct use by the pupils and that they do not receive inappropriate material.

A system backup is made every day.

Anti-virus protection is used to reduce the chance of infection via the Internet or email.

A regular search will be made for any executable or zip files. These will be deleted.

The transfer of files by USB sticks, by pupils, between network and non-network computers (eg home computers) is strictly prohibited. Staff may do so, only if they can guarantee that their computer if completely virus free and protected by anti-virus software.

An inventory is kept of all computer equipment and software.

All hardware is maintained by service agreements.

Software

The use or loading of software onto any of the computers on the network is prohibited without the permission of the ICT Co-ordinator.

Games may not be loaded or played on any computer, unless approved by the ICT Co-ordinator for training or teaching purposes.

Only the ICT Co-ordinator may load executable programs from a CD-ROM, USB stick or the Internet.

Printers

Pupils are only permitted to use the printers for authorised school work, with permission of a member of staff.

Laptops

Pupils are permitted to bring their own laptops into school only if written permission has been given by the Headmaster.

INTERNET ACCESS

All users

Access to the Internet is not a right, it is a privilege. Adherence to certain guidelines, rules and protocols is essential from all users. The Chorister School has certain expectations, laid out in this document, of users with regards to their responsibilities. The School's Internet access is made available to users for research and communication with others, but this is only on the understanding that you agree to follow the guidelines shown below.

The Chorister School has installed Wi-Fi throughout the school and purchased a set of iPads. With these latest technological advancements, it is important that The Chorister School remains vigilant to the threats posed by radicalisation and potential contact with terrorist groups. To counter these threats, The Chorister School has put in place the following measures:

1. No child will know the Wi-fi password and it will be changed regularly.

2. No child will have unsupervised access to the Wi-fi or iPad devices.

3. In ICT lessons, all children will be taught the SMART principles of Internet Safety as suggested by Childnet.

4. All children will be reminded of what they should do, should they see something inappropriate or which makes them upset on the internet.

5. Internet access is monitored by Total Business Group and they have put in place stringent filters on computers that can be accessed by children.

6. Staff have a wider access to the Internet on their machines, to access appropriate teaching materials. Their Internet usage is still monitored by Total Business Group.

7. Internet enabled smart watches (eg Apple Watch) are treated in the same way as mobile phones and must be handed in at school at Reception; they are not to be on a child during the school day.

Parents and Children

The Internet has enormous benefits when used sensibly. The School makes every effort to ensure the pupils are protected from inappropriate material, be it images or text.

The Internet is provided for users to conduct recognised school work only, except during the evenings, when boarders may access sites of more general interest with permission of the boarding housemistress.

All Internet access must be during staff supervised sessions. Boarders are permitted to use the Internet during leisure time, but also with staff supervision.

Prohibited Actions

Accessing, or trying to access, sending or displaying any obscene or offensive material.

Using inappropriate language, as in other parts of the School.

Releasing personal information about yourself or others – eg home address or phone numbers. Downloading games or other files with a .exe extension.

Private use of the internet or email service without prior permission of the Headmaster or if a boarding pupil, the Boarding House staff.

Undertaking financial transactions.

Accessing Chat Rooms or Instant messenger applications.

Internet audio and video streaming.

Internet games sites unless given permission by a member of staff.

Breaking of Copyright laws

Using a social networking site, e.g. Facebook, Instagram, Twitter etc. – exception for Boarders who are aged 13 and over and where this is allowed by the Boarding House and parents

Check with the ICT Co-ordinator before

Opening unidentified email attachments

Completing any online forms or questionnaires

See the ICT Co-ordinator if

You access any inappropriate material inadvertently or you receive a virus warning.

ICT SUITE USE

The ICT suite and other computers around the school are a resource for everyone. However there have to be certain rules to stop it being abused. These rules mostly concern the use of the Internet and printing.

The following rules therefore apply.

- Pupils may only use the ICT Suite during lesson time, break times and in the evening if a member of staff is there to supervise them continually and permission has been given.

- General school rules apply as much in the ICT Suite as in any part of the school.

- Eating and drinking are prohibited near any computer.

- Any member of Staff can remove the privilege of using the ICT Suite if a pupil does not follow the guidelines.

- Pupil use of the Internet is restricted to educational use during school time.

- Pupils may only print material if a member of staff has given permission.

These rules are set up to ensure that pupils do not misuse the system, and that school staff and parents can be reassured that their children are not gaining access to material that they may consider inappropriate.

Mobile electronic devices

Definitions

Handheld devices include; iPods, gaming devices, mp3 and mp4 players, PDAs, mobile phones, internet enabled smart watches. This list is not exhaustive and will expand as technology dictates.

Purpose

The widespread ownership of 'mobile phones and devices' (referred to as mobile devices) among young people requires that school administrators, teachers, pupils, and parents take steps to ensure that mobile devices are used responsibly at schools. This Acceptable Use Policy is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring that the benefits that mobile devices provide (such as increased safety) can continue to be enjoyed by our pupils.

The Chorister School has established the following Acceptable Use Policy for mobile devices that provides teachers, pupils and parents guidelines and instructions for the appropriate use of mobile devices at all times while our prep school pupils are on school premises or under the School's jurisdiction. Pre-Prep pupils should not have a mobile device.

Pupils, their parents or guardians must read and understand the Acceptable Use Policy before pupils are given permission to bring mobile devices to school.

Rationale

The Chorister School acknowledges that parents may give their children mobile devices to protect them from everyday risks involving personal security and safety, particularly those who travel to school independently.

With the continuing advances in technology and its applications, the School recognises that mobile technology can support pupils' learning and effective teaching.

The School acknowledges the importance to boarders of mobile devices as a means of communication with parents with whom pupils have limited access during term time, but equally the fact that these devices can raise problems specific to the boarding environment.

Responsibility

It is the responsibility of pupils who bring mobile devices to school to abide by the guidelines outlined in this document.

The decision to provide a mobile device to their children should be made by parents or guardians.

Permission to have a mobile device at school while under the school's supervision is contingent on parent/guardian permission in the form of a signed copy of this policy. Parents/guardians may revoke approval at any time, as may the School in the event of misuse.

Acceptable Uses

Mobile devices (including internet enabled smart watches) should be named, switched off and handed in at the school reception on arrival and collected at the end of the school day. Exceptions may be permitted only in exceptional circumstances if the parent/guardian specifically requests it. Such requests will be handled on a case by case basis and should be directed to the Headmaster.

Parents are reminded that in cases of emergency, the School Office (0191 3842935) remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.

Boarders will be given the option of using their phone or internet enabled smart watch after the evening meal and before prep each evening, but parents may speak to their child using the school number or the payphone up until bedtime. If you need to contact your child urgently, you would call the Housemistress or the Housemother on duty. This may be done at any time in the day or the night.

Pupils should only ever use their own mobile devices. Staff are always on duty in the Boarding House when mobile devices are being used and staff can monitor the behavior of the children whilst respecting the right to privacy. Staff are trained to be alert to children sharing or accessing youth produced sexual imagery, known as sexting.

The School wifi may be accessed by boarders on their own devices once the device has been added to the School's list of approved devices.. The school's wifi can only be accessed on an approved device during restricted hours – namely 18.00 – 20.00 Monday to Friday and from 8.00 – 20.00 on Saturday and Sunday.

Boarders may only use their phones or watches to access 3G and 4G with the permission of staff, and in one of the common rooms or the dining hall when a member of staff is present.

Mobile devices should not be used in any manner or place that is disruptive to the normal routine of the school.

Pupils should protect their phone numbers by only giving them to friends and keeping a note of to whom they have given them. This can help protect pupils' numbers from falling into the wrong hands and guard against the receipt of insulting, threatening or unpleasant voice, text and picture messages.

Unacceptable Uses

Unless express permission is granted, mobile devices should not be used at all during the school day. The School does not believe that phones or internet enabled smart watches are necessary for children on trips, including travelling to sports fixtures. The only exceptions are when children are being collected from a fixture by their parent and the phone or internet enabled smart watch will be held by the member of staff until the child is collected, or when the children are travelling a long distance to a sports fixture or educational trip and there are at least two members of staff on the vehicle.

Boarders are not permitted to use mobile devices in dorm once it is time for quiet reading – the system of handing in and collection is designed to ensure this does not happen.

The Chorister School's Information Communications Technology policy dictates that pupils should not have unsupervised access to the internet.

Using mobile devices to bully and threaten other pupils is unacceptable and will not be tolerated. In some cases it can constitute criminal behaviour.

Mobile devices must not be used to photograph pupils, members of staff or the wider School community without their consent. Images should not be shared unless this has been vetted by a member of staff. No pictures or videos taken may be sent via email or message to others or posted anywhere online. No personal information about themselves or anyone else can be sent from school or posted online.

It is forbidden for pupils to "gang up" on another pupil and use their mobile devices to take videos and pictures of acts to denigrate and humiliate that pupil and then send the pictures to other pupils or upload it to a website for public viewing. It is a criminal offence to use a mobile device to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

Mobile devices are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow pupils, staff or visitors to the school.

Pupils must not possess mobile telephone numbers of staff.

Boarders who are 13 and over and have access to social media may only use this to communicate with friends not with them in boarding and they must not attempt to 'friend' members of staff or Governors or other adults who work at school.

Should there be repeated infringements of the above regulations, the responsible pupil may face disciplinary actions as sanctioned by the Headmaster or Deputy Head.

Theft or damage

Pupils should mark their mobile device clearly with their names before handing them in to the school reception at the start of a school day.

The School accepts no responsibility for replacing lost, stolen or damaged mobile devices.

The School accepts no responsibility for pupils who lose or have their mobile device stolen while travelling to and from school.

It is strongly advised that pupils use passwords and PIN numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other pupils, or if stolen). Pupils must keep their password / PIN numbers confidential. Mobile devices and/or passwords may not be shared.

Inappropriate conduct

Any pupil caught using a mobile device to cheat in exams or assessments will face disciplinary action as sanctioned by the Headmaster or Deputy Head.

Any pupil who uses vulgar, derogatory, or obscene language while using a mobile device will face disciplinary action as sanctioned by the Headmaster or Deputy Head.

Pupils with mobile devices listed may not engage in personal attacks, harass another person, or post private information about another person using SMS messages, email, or by taking/sending photos or objectionable images, or making phone calls.

Pupils using mobile devices to bully other pupils will face disciplinary action as sanctioned by the School – usually by the Deputy Head or Headmaster.

It is inherent in the nature of such activities that an offence of this nature taking place outside of School impacts upon those within it, and as a result, such offences are punishable within School for the safety of the School community.

Sanctions

A mobile device will be confiscated if it is used other than described in the Acceptable Use section.

As set out in the previous section, failure to heed the rules set out in this document may result in an alleged incident being referred to Head of Pastoral Care for investigation. In such cases, the parent or guardian would be notified immediately and a more serious sanction may be applied.

The School reserves the right to ban individual pupils or groups of pupils from bringing mobile devices on site.

REVIEW

This policy will be reviewed in January 2020.

Appendix A

Acceptable Use of I.C.T

Pupil name (print) ____

Parent/Guardian Permission

I have read and understand the above information about the appropriate use of ICT and the Internet at The Chorister School and I understand that this form will be kept on file at The Chorister School and that the details may be used (and shared with a third party, if necessary) to assist with identifying a device should the need arise (eg. if an allegation of inappropriate use has been made).

I agree not to deliberately upload or text anything that would cause offence to anyone at school

I have discussed the safe use of the ICT, and the list on Appendix B, with my child.

I give my child permission to use the Internet at the Chorister School and understand that my child will be responsible for ensuring that they use the Internet appropriately and correctly while under the School's supervision, as outlined in this document.

Parent/Guardian name (print) ____

Parent/Guardian signature____

Date

Appendix B

Pupil Acceptable Use of ICT

Agreement / E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details, such as my name, phone number or home address.
- ✓ I will never arrange to meet someone myself. If I need to meet with someone, I will ask my teacher to arrange the meeting for me and make sure that a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ I know that my use of ICT can be checked and that my parent/guardian will be contacted if a member of school staff is concerned about my e-safety.
- ✓ Prep School pupils only – **mobile phones, smart watches (that can connect to the internet or have a data contract) and other electronic devices**

  I will only bring a mobile phone or smart watch or other electronic device to school if my parents have completed and returned the 'Acceptable Use of Mobile Phones and Internet enabled smart watch' form. My phone or internet enabled smart watch will be named, switched off and handed to school reception/Boarding House on arrival at school. I may collect my phone or watch when I am leaving school or at allowed times in the Boarding house. I understand that if I breach the school rules on use of mobile phones and internet enabled smart watches my phone or internet enabled smart watch will be confiscated.

Pupil name ____

Pupil signature ____

Appendix C

Acceptable Use Of Mobile Phone and Internet enabled smart watch Contract Prep School Children

This page must be completed and returned to school to enable your child to bring a mobile phone, internet enabled smart watch or other electronic device to school.

Parent/Guardian Permission

I have read and understand the above information about appropriate use of mobile devices at The Chorister School and I understand that this form will be kept on file at the School and that the details may be used (and shared with a third party, if necessary) to assist with identifying a device should the need arise (eg if lost, or if the device is being used inappropriately).

I give my child permission to carry a mobile device to school and understand that my child will be responsible for ensuring that the mobile device is used appropriately and correctly while under the School's supervision, as outlined in this document. I will notify you if my child has a change of phone number.

Parent/guardian name (print) ____

Parent/guardian signature ____

Date ________________________

Pupil name (print) ______________________________________

Mobile phone number of pupil ______________________________

Pupil signature ______________________________________

Date ______________________________