Cheadle Hulme School

E-SAFETY PRACTICES

The E-Safety Policy and these associated practice and guidelines are applicable to all pupils (Junior School and Senior School), staff, parents/carers, volunteers, governors and others with access to or are "users" of School information and communication technology.

Contents:

Introduction to E-Safety

Cheadle Hulme School recognises the importance and relevance of digital technologies for both the educational and business spheres of the School. The Internet, information technologies and digital communication (referred to as "IT") are powerful tools, which open up new and exciting opportunities which can stimulate discussion, promote creativity, increase collaboration and promote effective learning.

However, the use of this technology has become a significant component of many safeguarding issues with "users" (i.e. pupils *and staff*) at risk *within and outside* the School.

Some of the dangers those using information and communication technology may face include:

- Inappropriate or offensive Internet use
- Online and offline threatening behaviour;
- "Trolling" – the trend of anonymously seeking to provoke outrage by positing insults and abuse online;
- Blackmail – include 'revenge porn';
- Cyberbullying – writing messages with the intent to cause distress or anxiety in a public place (e.g. Twitter, Instagram);
- Grooming / Online predation – causing or encouraging a child under the age of 18 to engage in sexual activity online or meeting them in person after online contact. This also relates to contact with extremists;
- Fake profiles or hacking accounts;
- Cyberstalking - use of the Internet or other electronic means to stalk or harass an individual, a group of individuals;
- Illegal or inappropriate file sharing and exposure to other obscene/offensive content;
- Tagging photographs with defamatory or negative comments;
- Sextortion - use of webcams for flirting and cybersex;
- Exposure to extremist materials – including terrorist propaganda.
- Hacking or virus transmission
- Log-in misuse and password sharing
- Unauthorised access to or disclosure of sensitive information

The breadth of issues within online safety is categorised by the Department for Education into three areas of risk:

1. Content: being exposed to illegal, inappropriate or harmful material;
2. Contact: being subjected to harmful online interaction with other users; and
3. Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Development of a Policy to Safeguard against Harm

As technology can often be the platform to facilitate harm, an effective approach to safety is required to protect the whole School community. The e-safety policy has been developed by an Online Safety Forum working group and IT Steering Group made up of:

- Deputy Head Pupil Progress and Welfare
- Director of Technology
- Second Master
- Deputy Head (Teaching & Curriculum)
- Junior School Deputy Head (Y1-3)
- Assistant Head (Academic)
- Head of Geography
- Technical Services Manager

- Senior Operations Manager
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Whilst the policy is designed outline the commitments to safeguard pupils, they are also relevant to all those working at the School and members of the wider School community who have access to and are users of School's IT systems - staff, volunteers, parents and carers, visitors, community users.

Consultation has taken place through a range of meetings and communications; to work with the whole school community in the use of technology and to establish mechanisms to identify, intervene in and escalate any incident where appropriate.

The issues linked to online safety are considerable and whilst technical measures and monitoring are an important part of the digital safety culture, it is only one part. This Policy should be read in conjunction with other School safeguarding policies and procedures, and in a holistic approach with e-Security and Information Governance:

- Safeguarding Child Protection Policy and Procedures
- Anti-Bullying Policy and Procedures
- Staff Code of Conduct
- Data Protection and Freedom of Information Policy
- E-Security Policy

In order to ensure that this policy is implemented effectively, the School adopts the use of Acceptable Use Policy Agreements for Governors, Staff and Volunteers and for pupils in the Senior School; those in the Junior School use IT in a supervised and teacher-led environment. The School regularly reviews whether the practices, procedures and agreements it has to support this policy remain effective and current.

Definition of "E-Safety"

As the expansion of the technology and digital communications allows us to communicate with others through the Internet, therefore it also allows communications with malicious users and the concerns about the threats to personal safety are often referred to as "web safety", "cyber-safety", "digital safety", "online safety", "e-Safety" or "Internet Safety".

"E-Safety" in CHS refers to the practice of maximising online personal security, the safe use of information and electronic systems and the means by which users are protected from its associated dangers.

E-Safety is inclusive of both fixed and mobile Internet; online and offline; technologies provided by the School (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems and digital video equipment); and technologies owned by pupils and staff, but brought onto School premises (such as laptops, iPads, mobile phones and other mobile devices and wearable technology).

Senior School Online Safety Charter

As a member of the CHS community I value the rights and responsibilities relating to Internet use:

I have the right:

- To use the Internet without the fear of bullying
- To report comments that I find unacceptable
- To tell someone if I feel uncomfortable about something I see online
- To say no if someone asks me to do something I do not want to do
- To know who I am talking to online
- To access websites that are appropriate for my age
- To use the Internet to learn
- To use the Internet to communicate with my friends
- To have control of images, videos and work that belong to me
- To keep my accounts private
- To be trusted

I have the responsibility:

- To access reliable and trustworthy websites
- To not plagiarise information I read on the Internet
- To treat others online as I would want to be treated
- To be aware of my own personal safety online and not exchange personal information with people I do not know
- To keep my accounts secure, to keep my passwords private and change them regularly
- To report bullying or abuse
- To post information responsibly remembering that everything I post can stay online forever
- To talk only to people I know online
- Not to bring a Smart Watch to school because I am not permitted to wear one during the school day.
- Not to sign up to online services until I am old enough to do so (13+ in most cases).
- To respect the privacy of others
- To think before I click

This Charter is contained within the Senior School Planner and has been drawn up by the pupils themselves.

Junior School Code of Conduct:

When using technology I will:

- Keep my log-in and password secret
- Not share my personal details, images or another person's data online
- Only visit websites and applications appropriate to the task
- Tell a teacher if I am worried about something online or something others are doing online
- Only use my own technology when I have permission to do so

Roles and Responsibilities

The Designated Safeguarding Lead (DSL), Caroline Dunn Deputy Head (Pupil Progress and Welfare), is responsible for online safety.

The designated member of the Governing body responsible for online safety is Catherine Boyd (Safeguarding Governor).

The designated member of the Governing body responsible for e-security is Martin Tyley (IT Governor).

The Technical Services Manager is Mark Smith.

Designated Safeguarding Lead

- Will be the School's "E-Safety Officer," be supported by the Director of Technology, be trained in online safety issues and be aware of the potential for serious child protection issues resulting from online behaviour.
- Will establish and review the School E-Safety Policy and Procedures in line with wider safeguarding responsibilities.
- Will lead the Online Safety Forum.
- Will provide training and advice for staff.
- Will liaise with the School Technical Services Manager to ensure the ongoing security and safe use of IT systems within the School.
- Will liaise with the Senior School Head of Wellbeing and Junior Leadership Team to oversee the provision of E-Safety education.
- Will liaise with the Heads of Year to oversee the provision of E-Safety education through School assemblies.
- Will communicate concerns relating to E-Safety with parents.
- Will provide information and education sessions for parents.
- Will receive weekly reports of suspicious searching activity and email alerts for serious concerns to monitor individual risks and to inform future developments.
- Will administer sanctions, as appropriate to those pupils who maliciously misuse IT systems.
- Will investigate any issues which relate to inappropriate use of IT and administer sanctions as appropriate.
- Will identify any trends which can be detected in relation to misuse of systems by pupils and identify ways of following up such concerns.

Governors

- The Safeguarding Governor will meet at least termly with the Designated Safeguarding Lead and online safety issues will be discussed as an integral part of the safeguarding agenda.
- The Governor will report to the Board about any specific issues relating to the implementation of this policy including major breaches of the appropriate practice.

Technical Services Manager

works within Technical Services to:

- Ensure that the School's E-Security infrastructure is secure and is not open to misuse or malicious attack.
- Provide all users who may access the School's network with a properly enforced password protection policy.
- Update and apply the School's filtering systems on a regular basis.
- Update and implement the School's monitoring software and systems on a regular basis.

- Keep up to date with online technical information in order to inform and update the Designated Safeguarding Lead as necessary.
- Ensure that the Designated Safeguarding Lead receives weekly reports of suspicious searching activity and email alerts of serious concerns.
- Liaise with staff who report any suspected misuse of IT systems.
- Report any misuse of IT systems to the Designated Safeguarding Lead.

The Head & Senior Leadership Team

- Has a duty of care for ensuring the safety (including e-safety) of members of the School community, though the day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead.
- The Head, Head of the Junior School and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- Monitors and evaluates the implementation of the School E-Safety Policy and Procedures.
- Ensures that staff are adequately trained about e-safety.

All Teaching and Support Staff

are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and the School's E-Safety Policy and Procedures.
- They have read and understand the IT Acceptable Use Policy Agreement for Governors, Staff and Volunteers.
- They secure any sensitive information used in their day to day professional duties.

In addition to the Acceptable Use Agreement, staff have a responsibility to:

- Report any suspected misuse of IT systems to the Technical Services Manager.
- Report any safety concerns to the Head of Year/DSL as appropriate.
- Report any inappropriate mobile phone use to the Head of Year.
- Report any E-Safety incident which may impact on individuals or the School
- Ensure all electronic communications with pupils, parents, carers, staff and others are professional and in line with guidance on the use of Email within School.
- Ensure that pupils understand their IT Acceptable Use Policy Agreement (as appropriate).
- Ensure that pupils understand School procedures in relation to the use of mobile phones, cameras and hand-held devices and report any associated concerns (as appropriate).
- Guide pupils to sites checked as suitable for their use in lessons (as appropriate).
- Deliver relevant Wellbeing lessons (as appropriate and as directed).

Pupils

- Those in the Senior School are asked to sign the IT Acceptable Use Policy Agreement for pupils when they understand their responsibilities in using the School IT systems.
- Are supported to understand the need to report abuse, misuse or access to inappropriate materials.
- Are asked to read and understand relevant sections of the School Planner which relate to appropriate behaviour online.

Online Safety Forum

The Online Safety group provides a forum that has wide representation from the School, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives.

Members of the Forum (along with the IT Steering Group) assist the E-Safety Officer with:

Click here to return to contents page

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

IT Steering Group

The School's IT Steering Group evaluates emerging technologies to inform the Senior Leadership Team.

Members of the Group (along with the Online Safety Forum) assist the E-Safety Officer with:

- Considering the educational/business benefits of new technologies
- Communicating the overall e-safety programme to staff.
- Advising on future direction of IT in relation to e-safety and undertaking a risk analysis informed by the risk assessment required by the Prevent Duty.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers are encouraged to support the School in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student / pupil records
- their children's personal devices in School

Visitors and Guests

Visitors are able to access the School Wi-Fi with their own devices in School. However, when connecting to our system, all visitors agree to a terms and condition statement relating to the use of their devices. Upon arrival at the School, visitors are provided with the instruction that they:

- should not use any form of electronic device within the School without the express permission of the member of staff coordinating the visit. This includes the use of mobile phones;
- should not use photography or video equipment on the School site unless agreed prior to the visit;
- may connect to the School WiFi, but this is provided at the discretion of the Technical Services via the authorised channels only.

Breaches to any of these instructions may lead to the visitor being asked to leave the School premises and, if appropriate, external agencies consulted.

Guidelines for Safe Practice

Safe practice encourages pupils, staff and parents to engage with technology in a productive, positive and safe manner. These procedures and documented practices (as supplements to the overall e-Safety Policy) outline the School's e-safety culture and how IT activity is regulated within School; whilst providing guidance on ways of promoting appropriate/safe usage.

It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential so an education in e-safety is an essential part of an e-safety culture.

In order to ensure that different members of the School community are aware of their responsibilities, the use of computing and networking facilities is only permitted on the condition that all users sign to comply with the conditions stated in the Acceptable Use Policy Agreement.

School-Wide Education and Training

As a reference point, these Policy documents are available on the School Website for parents/carers, staff and pupils to access. Rules relating to the School Code of Conduct are displayed in the pupil School Planner and around School.

To establish an e-safety culture, turn this policy into practice and to ensure that the whole School community are provided with the education and resilience needed to protect themselves and their peers from online dangers:

1. E-Safety is **integrated into the curriculum** in any circumstance where the Internet or technology are being used, and during discrete Learning 4 Life and Wellbeing lessons, where personal safety and responsibility are discussed.

2. The School's **Wellbeing programme** is designed to educate pupils on the benefits and dangers of online use and encourage them to develop those characteristics which enable them to be responsible online, resilient if something goes wrong and have the courage to report and gain support when further help may be needed.

3. Through a fully embedded **digital learning programme**, pupils discuss the benefits, limitations and potential dangers of technology – including how to identify spam, phishing and virus emails and attachments; as well as how to be careful not to reveal any personal information, or arrange to meet up with anyone who they have met online that they do not know.

4. Pupils are educated on the use of social networking sites in safe and productive ways.

5. **Assemblies** are used as a vehicle for teaching pupils about responsible online use and strategies to avoid associated dangers.

6. The Senior School **Daily Bulletin** is used to remind pupils of the importance of resilience when facing online challenges.

7. With so much information available online, pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the School as part of **digital literacy** across all subjects in the curriculum. Pupils are taught to:

    - be critically aware of materials they read, and shown how to validate information before accepting it as accurate;
    - use age-appropriate tools to search for information online;
    - acknowledge the source of information used and to respect copyright.

Click here to return to contents page

Plagiarism is against the law and the School takes any intentional acts of plagiary very seriously. Pupils who are found to have plagiarised are disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

8. E-Safety is considered part of the wider School strategy in relation to safeguarding and staff receive information relating to online dangers in their bi-annual **mandatory safeguarding training** and other update training ("Know Your Responsibilities").

9. There is an on-going digital-safety **awareness campaign** to all staff and students covering essential e-safety procedures and modern cyber security – including themed weeks/classroom topics.

10. Safe and professional online behaviour for staff is discussed at **in-sessional training days**.

11. New users are made aware of their personal responsibility to comply with the IT security policies as part of their **induction process**.

12. The School takes every opportunity to help parents understand these issues through parents' evenings, **newsletters, letters, website** and information about national / local e-safety campaigns / literature.

13. **External training** is made available for staff to ensure they are informed of the most up to date guidance (through a cluster of e-learning modules from The Tech Partnership).

14. As Champions of a safe online lifestyle, staff are encouraged to stay informed by reviewing **external websites** such as The UK Government-sponsored Get Safe Online website, The UK Government Cyberstreetwise website and Microsoft's Safety and Security Centre website.

Click here to return to contents page

Good Password Security Practices

A safe and secure username and password system is essential to help maintain the security of the School network, data, and systems – reducing online safety risks. All pupils, staff, parents/carers, volunteers and governors are responsible for all activity that takes place under their CHS username, so although it may seem disruptive, changing passwords frequently is good security practice.

Key groups and users are frequently prompted to change their School network password when logging on to a School computer. The new password will automatically work for integrated CHS systems (those accessed by staff such as iSAMS, Schoology, Room Booking System, VOLE, Webmail etc.). All users are encouraged at this frequency to change their passwords for other 'standalone' systems or databases.

All users have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Within the Junior School, a pragmatic approach is taken to store infants and junior pupils' passwords centrally – but any document is password protected and accessible only by the Junior Leadership Team.

Accounts are "locked out" following six successive incorrect log-on attempts. Anyone requiring assistance with managing passwords (or to reset a password) are guided to contact Technical Services who will ensure that full records are kept of usernames and any security incidents related to this saucer practice.

Passwords for new users, and replacement passwords for existing users are allocated by Technical Services. Members of staff are made aware of the School's password policy at induction and through the Acceptable Use Agreement. Pupils are made aware of the School's password policy through the Acceptable Use Agreement, in assemblies, in e-safety sessions and through the use of posters placed around School.

Options are available to change passwords from School computer and remotely.

All School user accounts follow the password guidelines below:

Infants and Junior School Students

- Minimum of 4 characters
- It should not contain any personal information (name, user name, or reference Cheadle Hulme School etc.)
- Change every 12 months
- Can't use previous 3 passwords

Staff, Senior School Students, and 'System' accounts

- Minimum of 8 characters, and include three of – uppercase character, lowercase character, number, special characters
- It should not contain any personal information (your name, user name, or reference Cheadle Hulme School etc.)
- Change every 6 months
- Can't use previous 3 passwords

System Administration and High Risk Groups

- Minimum of 12 characters, and include three of – uppercase character, lowercase character, number, special characters
- It should not contain any personal information (your name, user name, or reference Cheadle Hulme School etc.)
- Change every 3 months

- Can’t use previous 3 passwords

High Risk Groups are those with access to sensitive and personal information such as those in First Aid, Learning Support, Student Managers, Examinations team, Human Resources, Senior Leadership Team, Executive Assistant to the Head, Bursary team, Technical Services, IT Steering Group. These users are required to change their password more frequently.

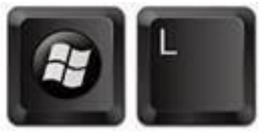
Considering how much the School relies on mobile devices (iPads, laptops), and how susceptible they are to attack, all mobile devices and personal equipment used to access the School network/systems should be secured with a Touch ID or minimum 4-digit passcode (mobile device/tablet), or 8-digit password (desktop computer/laptop).

The “save password option” should not be selected in applications as it means accounts can be misused.

Mobile devices should be set to lock automatically after 5 minutes of inactivity and never left unlocked whilst unattended.

To protect School owned IT and access to information systems, all networked computers are set to auto-lock after 20 minutes of inactivity. A password is required to regain access.

Quick tip: to lock computers when away, simultaneously press the 2 keys below:



Anyone who has disclosed their password or thinks their account has been compromised, should change their password immediately by pressing Ctrl, Alt and Delete keys, select Change Password option, then following the on-screen instructions. Anyone who thinks their account may have been maliciously compromised, are required to notify Technical Services of their concerns.

Safe Use of Mobile and Wearable Technology

Mobile communication devices (such as iPads or other tablet computers and Chromebooks) and wearable technology (such as Apple Watches and Google Glass) are part of everyday life. We aspire to teach pupils to recognise the educational value of using a personal device in a safe, controlled and creative manner and to support the whole School community we have a responsibility to educate staff on how to use them responsibly and safely.

Mobile and wearable devices are fantastic technology but can:

- make pupils and staff more vulnerable to cyberbullying;
- be used to produce and send Youth Produced Sexual Images (sexting);
- be used to access inappropriate Internet material;
- be a distraction to learning
- have integrated cameras, which can lead to child protection, bullying and data protection issues;
- be stolen, vandalised and maliciously abused.

Smart watches and other wearable technology are not permitted for School activities at any times.

! *Anyone who brings a mobile phone or personal device into School is a responsible for its safe keeping and insurance. The School will not take responsibility for personal devices that have been lost, stolen or damaged.*

Mobile Phones

During the course of the School day, there is no need for any pupil to have use of a mobile phone. The pastoral system (Form Teachers, Heads of Year, Heads of School and Student Managers, and the Medical team), means that every pupil is able to contact home if needed; with a fully staffed Reception desk, parents are able to contact their son and daughter between 8.30am and 3.45pm should this be necessary.

Many pupils have unlimited and unrestricted access to the internet via 3G and 4G so with this in mind, mobile phones are banned in the Senior School for Years 7 to 11 between the hours of 8.30 and 3.45pm. Pupils seen using a phone during these times (or wearable technology at any time) will be given an automatic lunch time detention.

- For the Junior School, mobile phones should be handed in on arrival in the classroom in the morning and then collected at 3.30 pm.

- Pupils in Year 7 – 9 must hand in their mobile phones to their Form Tutors during morning Registration. The devices are redistributed at the end of afternoon Registration. When returned to the pupils, devices remain off and should be safely stored for the rest of the day.

- Pupils in Years 10 and 11 safely store their mobile phones between the hours of 8:30am and 3:45pm.

- Sixth Form Pupils will not be able to use their personal devices as they move around the site but are permitted to respectfully and responsibly use them in the Sixth Form Common Rooms – providing they do so within the requirements of the User Agreement.

The following rules also apply to the use of mobile phones:

- Pupils must not use their mobile phone to contact parents/carers if they are feeling unwell. First Aid will make the decision as to whether a pupil is well enough to stay in School and will contact parents/carers as necessary;

- Pupils must not take photographs or film others in School or those wearing a CHS School uniform without the explicit permission from a member of staff; and those being captured;
- When permitted to use their phone, all pupils are required to do so *responsibly* and within the requirements of the signed User Agreement.
- Pupils must not use it to send unpleasant messages or engage in malicious gossip. Such behaviour will be regarded and treated as bullying.

Personal Devices for Learning

We are very excited about using digital learning to empower our students to become leaders of their own learning. The School is increasingly using Chromebooks, iPads, Laptops and other mobile technology to enhance teaching and learning and for some Senior School Year Groups is it compulsory to have a digital device in classes; with others it is still encouraged.

Such devices will be used in lessons at the direction of the teacher for educational purposes only; they should not be used for any other reason for recreational purposes nor whilst moving around the School site.

If pupils wish to use their devise for academic purposes during their free time, they must go to the Library where their activities can be supervised.

No pupil may use the camera / video function of any mobile device without the explicit permission from a member of staff. Any images or films allowed should not be sent between mobile devices without explicit permission from a member of staff.

Staff Personal Devices:

- Staff should not use their own personal devices to contact pupils or parents/carers either in or out of School time. In the event of this happening they must report the matter to the Designated Safeguarding Lead or the Head via the Note of Neutral Notification.
- Staff should not take photos or videos of pupils on personal devices. If photos or videos are being taken in a professional capacity they will inform the Designated Safeguarding Lead and download and delete the pITures as instructed (including any cloud storage spaces). Legitimate recordings and photographs will be captured using School- monitored equipment such as cameras and iPads.
- Staff are expected to lead by example; personal mobile phones should be switched off or on 'silent' during School hours and should not be used in a space where pupils are present (e.g. classroom, playground).
- Staff and visitors must not use any personal digital device in any part of the Early Years Foundation Stage setting.
- Members of the Senior Leadership Team and the Critical Incident Team are encouraged to carry their mobile phone with them simply for use in the event of a School emergency.
- In circumstances such as outings and off site visits, staff can book out a mobile phone but where this is not practical can agree with their manager the appropriate use of personal mobile phones in the event of an emergency (all other rules apply).

Misuse of Mobile Phone or Personal Devices

- Members of staff can confiscate a pupil's mobile device and a member of the pastoral team can search a pupil's device if there is reason to believe that there may be evidence of harmful or inappropriate use.
- Pupils may not, under any circumstances, bring mobile phones or personal devices into examination rooms. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Use of Identifiable Recordings and Images

Generally, photographs and videos taken in School are used legitimately for teaching purposes, for academic celebrations and for a sense of Waconian pride. For everyone's safety due to the potential misuse of photographic images and recordings (printed, digital and video) and concerns about the publication of personal data, we are proactive in our management of the capturing, storage and use of identifiable recordings and images.

- On admission to the School parents/carers sign a Parent/Carer Contract which asks them to inform the School if they do not wish for images of their child/children to be taken.
- Parents/Carers are able to withdraw or restrIT this consent in writing to the Head at any time.
- Otherwise parents/carers consent to the taking of photographs, images and film or video recordings of the pupil for use in the promotional literature of the School or on its website or in social media, to publicise the School's activities by the School in the media, or as a memento or record of pupils at the School.
- Parents wishing to raise concerns over potential misuse of photography or video can do so by following the usual Parental Complaints Procedure.

Publishing Photographs and Videos with Identifiable Personal Data

Safety principles for publishing photographs and videos with identifiable personal data:

Images and videos should not identify pupils or put them at risk of being identified:

- ✗ Image/film
- ✗ name, and
- ✗ location

of any individual pupil should never be published together.

Only images created by, or for, the School will be used in public and pupils will not be approached or photographed while in School or doing School activities without the School's permission.

The School follows general rules on the capturing, storage and use of digital recordings and images of pupils:

- Any members of staff taking photographs or films at events wear CHS ID badges.
- Staff comply with Data Protection legislation when storing images of pupils.
- Images are be carefully chosen to ensure that they do not pose a risk of misuse. (this includes ensuring that pupils are appropriately dressed);
- For public documents, including newspapers, full names are not be published alongside images of the child. Groups may be referred to collectively by Year group or Form name;
- Any professional Photographers that are arranged by the School are fully briefed on appropriateness in terms of content and behaviour. Staff are informed at least two weeks prior to a Photographer arriving, who will wear identification at all times.
- No photography or filming is permitted to take place in unsupervised areas (for more information on safeguarding in School please refer to our Safeguarding CP Policy and Procedure);
- If other organisations or visiting schools wish to take pITures, they can only do so with the explicit permission of the supervising member of staff and they must agree to comply with the above principles;

- Children in Early Years Foundation Stages will not be photographed other than by members of staff and using School devices for educational purposes only;

Photography and Videos at School Events

Visitors to the School, including parents and carers, are informed not to take images of pupils at School events – without explicit permission from the supervising member of staff and must agree to comply with the above data protection principles.

When pupils from other schools are involved in an event:

  - Photographs are only be taken when explicit permission has been received to do so from other schools; permission is sought by email from the other school(s) using the standard wording below:

Text to be sent to other schools to request permission to take photographs/film of their pupils during an activity:

We would like to take photographs and video of pupils taking part in (name of event) which will be taking place at (location) on (date). The primary aim is to take images of our own pupils for PR purposes, however the nature of the event means that some of your pupils may inevitably appear in the images. The images may be used for coaching purposes or on the Cheadle Hulme School website, the School magazine and, where appropriate, for sending to local media. We would never use an image of an individual pupil from your school and none of your pupils would ever be named.

Can you please confirm, by replying to this email, that you are happy for this to go ahead.

  - If permission is not received in writing then all staff involved in the event is made aware of this by the individual responsible for the event;
  - On Saturday mornings permission to photograph, or otherwise, is indicated on the hosting information sheet;
  - Any nominated photographers or official representatives will make themselves known to the member(s) of staff representing the other school before taking any pITures.

When other schools request permission to take photographs in advance of the event this will be considered either by the Head of Department, Designated Safeguarding Lead, or another member of the Senior Leadership Team (or Junior Leadership Team) and they will receive a reply containing the following wording:

Text to send to others when they have requested permission to take photographs/film of CHS pupils during an activity:

We give permission for official representatives of your organisation to take photographs and video of pupils taking part in (name of event) which will be taking place at (location) on (date). This is on the strIT understanding that the images will be used for coaching or PR purposes, that you do not use images of an individual CHS pupil and that none of our pupils would ever be named.

Can you please confirm, by replying to this email, that you are happy to abide by these conditions

Any requests on the day of the event not given prior consent is refused.

Any member of staff observing unauthorised pITures being taken they will inform a member of the Senior Leadership Team or Safeguarding team but if none are present they will (where practicable):

- Establish the identity of the individual (if not already known);
- Establish the purpose for which the images are being taken;
- Challenge individuals who are taking images of pupils without clear authority.

Online Media and Websites

The Cheadle Hulme School website is in the public domain and is a valuable resource for keeping up-to-date with School news and events, celebrating whole-School achievements and personal achievements, and promoting School projects. All information published on this website is carefully considered by the External Relations team in terms of safety for the School community, copyrights and privacy policies. No personal information about staff or pupils is published, and details for contacting the School is the School office numbers only.

Social Networking/Media and Personal Publishing

Regulated publishing tools such as blogs, wikis, social networking sites (Twitter, Facebook), bulletin boards, chat rooms and instant messaging are often used in School for promoting trips, special events and subject specific news and information. Responsible use of social media can be positive for learning and teaching; however, staff and pupils are made aware of the risks and responsibilities of creating a safe online environment and that once content is publicly published it leaves a "digital footprint".

Any sites that are used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

Official School blogs created by staff or pupils/year groups/School clubs as part of the School curriculum is password-protected and run from the School website with the approval of a member of staff and is moderated by a member of staff.

The following guidelines support members of staff in their safe online communications which can directly and indirectly, represent the School:

- Use caution in the use of social media and carefully consider the sharing of opinions or images that are likely to cause offence, compromise their role, cause embarrassment or discomfort to others, reflect poorly on their professional responsibilities or the reputation of the School;
- Do not request, or accept a request, to 'friend (or equivalent) current pupils and take caution in friendship links to past pupils, especially if these individuals have active family or personal relations within the School. (Refer to the Staff Code of Conduct for further guidance.)
- Ensure that personal online profiles are appropriately secured (ideally made private);
- Do not refer to professional roles in any capacity when using social media and add a disclaimer along the lines of "Opinions are my own and not the views of the School."
- Be mindful of how friends/followers can influence your reputation on social media;
- Do not give out personal details, such as mobile phone number, personal email address or social network account details to pupils, parents/carers;

Use of Email

Email is the cornerstone of most of our communication and has allowed us to be much more responsive and frequent in our dialogue, while at the same time enabling us to maintain effective records of any exchange. Email is a risky communication method;

Click here to return to contents page

contents can be easily misread, misunderstood, copied/screenshot, forwarded and posted online.

Members of staff and pupils only use official School-provided email accounts to communicate with each other (and with parents or carers). Personal email accounts should not be used for School communications. Staff emails should be professionally and carefully written in line with the Communication Style Guidelines.

As staff represent the School at all times, everyone is asked to take this into account when entering into any email communications by checking contents with respect to discrimination, harassment or defamation. By the same token, staff are asked to inform their manager, the Designated Safeguarding Lead or a member of the Senior Leadership Team if they receive any offensive, threatening or inappropriate emails.

Pupils are advised tell a member of the pastoral team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with these themselves.

Cyberbullying

The School takes any form of bullying, including cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Anti Bullying Policy and Procedures.

The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Spam, Phishing Emails and Identity Theft

Most people are aware that they should protect their information in real life, for example by shredding documents with financial or personal details. However, there are many ways fraudsters can gather this information from pupils and staff online.

Identity Theft

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit fraud or another malicious act. Identity theft can have a direct impact on personal wellbeing, finances, and reputation.

The whole School community is encouraged to prevent identity theft by following these simple tips:

- Do not open suspicious unsolicited emails – even to unsubscribe or ask for no more mailings; this just confirms your email address and you'll get more not less. Delete unsolicited emails and call Technical Services for advice on setting spam filters.
- Stop and use common sense - you wouldn't give bank details or a password to a stranger in the street, so don't give this information in response to an email (Technical Services will NEVER request your password in an email).
- Avoid posting images with personal information – such as vehicle registration, outside your front door with the number visible, pITure of documents with contain personal information (such as exam results letters);
- Do not open attachments or links in emails unless you were expecting the email - delete the email.
- Check that websites are secure before entering personal or financial details.
- Enhance your privacy settings on social networks

The School’s email system incorporates advanced security features, but it is important to understand that email security features are never guaranteed to detect all malicious or otherwise-undesirable emails; it is therefore vital that users remain vigilant when handling incoming emails.

Spam

Spam email is the electronic equivalent of junk mail. The term refers to unsolicited, and often unwanted material which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself. Spam emails may feature some of the following warning signs:

- You don’t know the sender.
- Contains misspellings designed to fool spam filters.
- Makes an offer that seems too good to be true.
- The subject line and contents do not match.
- Contains an urgent offer end date (for example “Buy now and get 50% off”).
- Contains a request to forward an email to multiple people, and may offer money for doing so.
- Contains a virus warning.
- Contains attachments, which could include .exe files.

Phishing emails

Phishing is a scam where criminals typically send emails to thousands of people. These emails pretend to come from banks, credit card companies, online shops and auction sites as well as other trusted organisations. They usually try to trick you into going to the site, for example to update your password to avoid your account being suspended. The embedded link in the email itself goes to a website that looks exactly like the real thing but is actually a fake designed to trick vITims into entering personal information.

The email itself can also look as if it comes from a genuine source. Fake emails sometimes display some of the following characteristics, but as fraudsters become smarter and use new technology, the emails may have none of these characteristics. They may even contain your name and address.

- The sender’s email address may be different from the trusted organisation’s website address.
- The email may be sent from a completely different address or a free webmail address.
- The email may not use your proper name, but a non-specific greeting such as “Dear customer.”
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character’s difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email may be contained within an image rather than the usual text format.
- The image contains an embedded link to a bogus site.

Illegal file sharing

Peer-to-peer file sharing is the distribution and sharing of digital media using peer-to-peer (P2P) networking technology. BitTorrent is a communications protocol of P2P file sharing which is used to distribute data and electronic files over the Internet.

In both cases, hosts store files on their computers and the file-sharing software enables other users to download the files onto their own computers. Many people utilise P2P file sharing software (such as KaZaA, Gnutella, and FreeNet, among others) but downloading material where you have not obtained the copyright owners permission is not only against the School's IT Acceptable Use Policy Agreement, it is against the law.

Using torrent or other P2P file sharing software to obtain films, music, games or software which are not paid for, is theft. While there are exceptions, 95% of material on torrents is not obtained legally, and therefore use of peer-to peer systems on the School network is prohibited and blocked.

By default, P2P applications will search for and share content from computers, they usually run as soon as the computer is turned on and continues to run in the background so this software can undermine the network security and expose the School to threats, such as viruses, malware, password and identity theft, spyware.

Lawyers for copyright holders (usually movie or music producers) watch P2P sites to see who is advertising their protected material and so use of these P2P file sharing or torrent software will result in user accounts being blocked until users agree to:

- Stop using a School network for file sharing activity;
- Delete any offending software from the computer - if you have P2P file sharing applications installed on computers, you may be sharing copyrighted works illegally without even realising it;
- Not install further P2P file-sharing software on any School computer;

If illegal activity continues after this time, further breaches of the IT Acceptable Use Policy Agreement will subject to a Disciplinary Procedure.

Removable Media Controls

Removable media are any devices which can be used for mobile computing either in their own right or by being connected to and removed from other computing devices. The use of removable media (for example, USB memory "sticks", flash drives, smart phones, external hard drives, media card readers and other personally owned devices) can import malicious content either intentionally or accidentally into the School's IT infrastructure that might compromise personal safety and/or sensitive information.

The following risks are associated with poor control over removable media:

- Disclosure of information as a consequence of loss, theft or careless use of removable media devices.
- Contamination of School networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.
- Potential sanctions against the School or individuals imposed by the Information Commissioner's Office as a result of information loss or misuse.
- Potential legal action against the School or individuals as a result of information loss or misuse.
- Reputational damage as a result of information loss or misuse.

To control these risks, the School prohibits the use of all removable media devices as a default mechanism for storing or transferring information. Access to media ports are denied by default, only allowing access to approved users or specific hardware. Non-compliance with this safe practice could have a significant effect on the School's ability to maintain security of the computer network.

Under normal circumstances information will be stored on School network systems or exchanged using appropriately protected mechanisms such as the School-recognised cloud-based sharing platforms such as OneDrive, GoogleDrive and Schoology.

Click here to return to contents page

Where the use of removable media is required, it will be limited to the minimum media types and users needed and it will need to be demonstrated that clear business benefits outweigh the risks before approval is given (by the Technical Services Manager). Requests for access to, and use of, removable media devices are made to Technical Services and will be automatically scanned for malware when it is introduced to the School system. Any School data stored on removable media devices will be protected by encryption software and with password protected auto locking features enabled (where present).

Where removable media is to be destroyed or no longer used for School-use, to avoid data leakage, appropriate steps will be taken to ensure that previously stored information is no longer accessible.

Filters and Authorised Monitoring

Through the Technical Services infrastructure, appropriate filters and monitoring systems will be put place:

- Technical Services' authorised staff may inspect any IT equipment owned or leased by the School at any time without prior notice.
- Technical Services' authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, Internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.
- Technical Services' authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.
- All monitoring, surveillance or investigative activities are conducted by Technical Services authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
- Personal communications using School IT may be unavoidably included in any School communications that are monitored, intercepted and/or recorded.

Monitoring of Email:

- Automated email monitoring and blocking systems are in use.
- Incoming and outgoing emails may be read at any time by authorised monitoring staff.
- The School reserves the right to retrieve the contents of email and other files when a member of staff is absent for the purposes of determining whether the use is legitimate, to find lost messages or retrieve messages following computer failure, to assist in the investigations of wrongful acts or to comply with any legal obligation.

Safety Breaches and Incident Reporting

The School will take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. Regular software and broadband checks take place to ensure that filtering services are working effectively. Any material found by members of the School community that is believed to be unlawful will be reported to the Designated Safeguarding Lead who will refer to the appropriate agencies..

A breach or suspected breach of this safe practice may result in the temporary or permanent withdrawal of School IT hardware, software or services from the offending individual.

Click here to return to contents page

- Pupils who breach the Acceptable Use Agreements in relation to their personal devices may be disciplined in line with the School's Behaviour Policy.
- Pupils who breach the Acceptable Use Agreements in relation to their personal devices may face disciplinary action in line with the School's Staff Disciplinary Procedure.

Breaches may also lead to criminal or civil proceedings.

! Any **security breaches** or attempts, loss of equipment, virus notifications, unsolicited emails and any other unauthorised use or suspected misuse of IT must be immediately reported to **Technical Services**.

! Any **safety or safeguarding concerns** must be immediately reported to the **Designated Safeguarding Lead**.

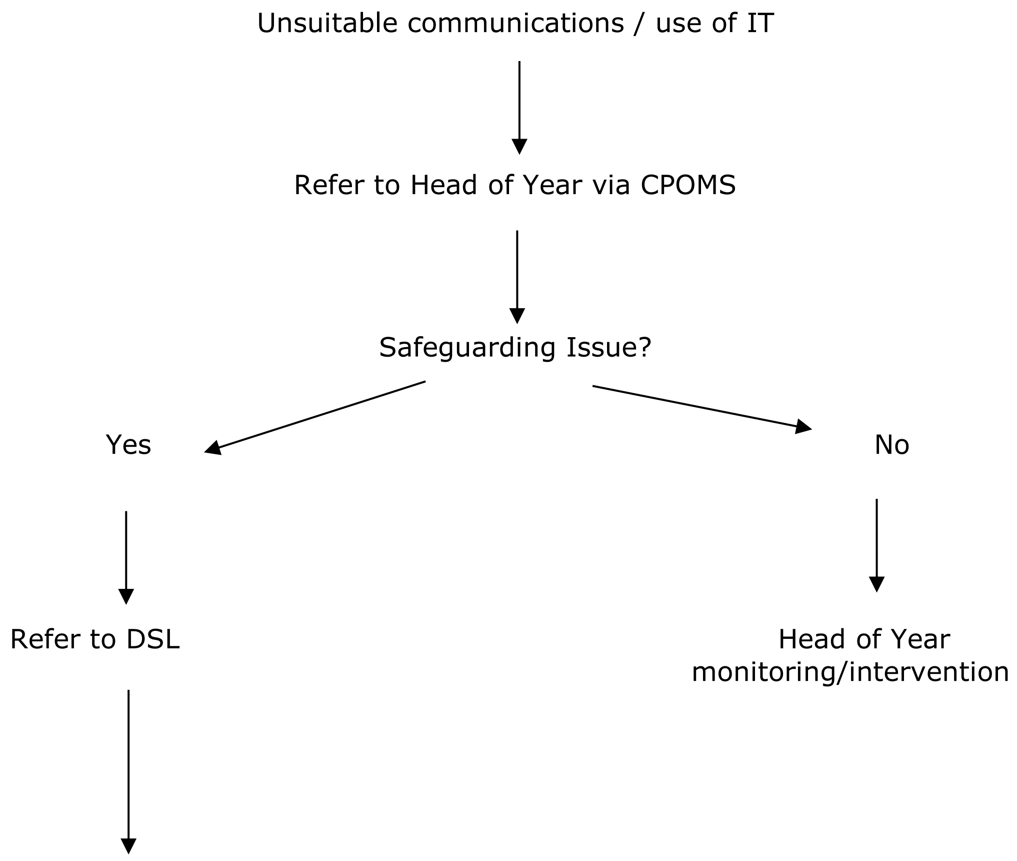
To maintain a strong culture of e-safety, an effective incident reporting culture and a regular dialogue between users and the Safeguarding and/or Technical Services team is crucial. This reporting culture is essential to uncovering potential risks or areas where technology and processes can be improved, as well as identifying actual incidents.

The most effective defence to an incident is achieved through awareness and the safe working practices. . The flowcharts in Appendix 3 & 4 summarise the procedures used to report issues and concerns relating to E-Safety.

Approved by Head & Second Master:	June 2017
Proposed Review Date:	June 2020
SLT Member Responsible:	Deputy Head PPW

Click here to return to contents page

Procedures for dealing with e-Safety Reports


Unsuitable communications / use of IT
Refer to Head of Year via CPOMS
Safeguarding Issue?
Yes
No
Refer to DSL
Head of Year monitoring/intervention

1. DSL to investigate
2. DSL to liaise with parents
3. DSL to sanction as appropriate (in conjunction with the Head if sufficiently serious to warrant suspension/expulsion)
4. DSL to contact police if any evidence of criminality/see YPSI guidance
5. DSL to record in bullying log if appropriate
6. DSL to identify potential trend
7. DSL to advise regarding follow up (wellbeing provision/assembly)

Click here to return to contents page

Illegal materials or activities found or suspected

Refer to DSL/secure and preserve evidence

Assess level of risk

DSL to contact LADO (if connected to member of staff) / Police and proceed as advised
Proceed with internal procedures if receive advice of no illegality / threshold having been met

Depending on advice received

1. DSL to record
2. DSL to identify potential trend
3. DSL to consider possible follow up needed

Click here to return to contents page

Cheadle Hulme School

ICT Acceptable Use Policy Agreement (Governors, Staff and Volunteers)

This Agreement details the professional responsibilities all Governors, staff and volunteers need to be are aware of when using any form of IT in School. All users are expected to read the E-Safety Policy and Practice document and sign this Agreement as an indication they will adhere to their e-safety and e-security responsibilities at all times.

Any concerns or clarification should be discussed with the Deputy Head Pupil Progress & Welfare.

As a member of the Governing Body / a member of staff / volunteer I confirm that I:

- will only use the School's email/Internet/intranet/Learning Platform and any other related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body;
- will comply with the IT system security culture and not disclose any access information provided to me by the School or other related authorities;
- will ensure that all electronic communications with pupils, staff; parents and other professional bodies are compatible with my professional role;
- will not provide my own personal details such as mobile phone number; personal email address; personal Twitter account, or any other social media link, to pupils;
- will only use the approved, secure email system(s) for school business;
- will ensure that personal data (e.g.as held on MIS software) is kept secure and is used appropriately, whether in School, or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off-site will be encrypted, e.g. on a password secured lap-top or cloud storage system;
- will not install any hardware or software without permission;
- will not use personal electronic devices and wearable technology, in public and teaching areas of the School between the hours of 08.30 and 15.45.
- will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;
- will not take, store or use images of pupils and/or staff unless in line with School safe practice;
- will not distribute images outside the School network unless in line with School safe practice;
- understand that my use of the School's Internet, systems and other related technologies will be monitored;
- will respect copyright and intellectual property rights;
- will ensure that my online activity, both in school and outside school, will not bring the School, my professional reputation, or that of others, into disrepute;
- will support and promote the School's E-Safety culture along with e-Security Policies other data protection practices and help pupils be safe and responsible in their use of IT and related technologies;

Click here to return to contents page

- will report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I agree to follow the safe practices as detailed in the E-Safety Policy and Practice document and to support the safe and secure culture of IT use throughout the School.

Name ______________________________

Signed ______________________________

Date ______________________________

Click here to return to contents page

Acceptable IT Use Agreement and Senior School Pupil Code of Conduct

School Policy:

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The School will try to ensure that students will have good access to digital technologies to enhance their learning and, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement:

I understand that I must use School IT systems in a responsible way, to minimise risk to my safety or the safety and security of the IT systems and other users.

Please read this Agreement carefully; if you have any questions, please refer to a member of staff. You will be asked to acknowledge your acceptance of this Agreement annually.

For my own personal safety:

- I understand that the School will monitor my use of the School's IT systems, devices and digital communications to ensure that I am using the technology safely and appropriately.
- I will only access the School's IT systems using my School account, authorised account and password;
- I will keep my username and password safe and secure and will not use another person's password. I understand that I should not write down or store a password where someone else may have access to it;
- I will be aware of 'stranger danger' when I am communicating online;
- I will not disclose or share personal information about myself or others online (this includes names, addresses, email addresses, telephone numbers, age, gender, school details, financial details and so on);
- If I arrange to meet people offline that I have communicated with online, I will do so in a public place and take an adult with me;
- I will immediately report to a member of CHS staff anything I see online that makes me uncomfortable or any unpleasant or inappropriate material or messages;

Use of the School Systems:

- I understand that the School's IT systems are primarily intended for educational use and I will not use them for personal or recreational use unless I have permission to do so from a member of staff;

- I am responsible for all access and files located within my 'Home Area', any files I upload to 'Shared Areas' and any documentation showing my username;
- I will only use the School printing facilities for academic work and School-related activities;
- Unless I have permission, I will not try to make large downloads (files in excess of 50MB) or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not use public chat rooms;
- I will not use the School's systems or devices for online gaming, online gambling, internet shopping, file sharing or video broadcasting or any other non-educational purpose unless I have explicit permission from a member of staff to do so;
- I will not upload, download or access any materials that are illegal, inappropriate or that may cause harm or distress to others, and understand that this includes any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent them;
- I will not install or attempt to install software of any type on any School device or try to alter computer settings;
- I will not attempt to introduce anything to the School network which could compromise the network security (e.g. malware, viruses, hacking software) and I will not attempt to access other user's files and folders without their permission
- I will only use social media sites with permission;
- I will immediately report any damage or faults involving equipment or software to a member of CHS staff, however this may have happened.

I act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- I will be polite and responsible when I communicate with others; I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will not take or distribute images of anyone without their permission;

When using the internet for research or recreation, I recognise that:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos);
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of other may not be truthful and may be a deliberate attempt to mislead me.

Using my own device (One-to-one Mobile Digital Devices):

- I take full responsibility for my device and understand that the School is not responsible or liable in respect of lost, stolen or damaged devices whilst at School or on activities organised or undertaken by the School (the School recommends insurance is purchased to cover the device whilst out of the home)
- I will only use my own personal devices (eg mobile phone / USB devices / iPad) in School when I have permission. If I do use my own device(s) in School, I will follow the rules and Code of Conduct set out in this Agreement, in the same way as if I was using School equipment and in

line with School policy.

- I will ensure my device is secured with a password/passcode, has a protective cover and is identifiable as mine;
- I will only access files, internet sites or apps which are relevant to the academic curriculum;
- I will only use my device in designated teaching and learning areas and not when I am moving around the School site;
- I understand that the device's camera is prohibited unless authorised by the teacher; I must only photograph people with their permission. I will only take pictures or videos that are required for an educational task or activity. All unnecessary images or videos will be deleted immediately;
- I will never use my digital device in toilets or changing rooms or other potentially sensitive environments
- I will ensure my device is sufficiently charged, with enough power to last the whole school day, before bringing it into School;
- I will keep my device on silent on the School site and on School buses;
- I understand that the School has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate;
- I will keep my device secure and up to date through software, security and app updates.
- I must not attempt to bypass the School's network filters which will be applied to my connection to the Internet
- I will abide by the mobile phone policy appropriate to my year group
- **I understand that I am responsible for my actions both in and out of School:**
- I understand that the School has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this Agreement, when I am out of School and where they involve my membership of the school community (e.g. cyber-bullying, sharing of images or personal information.)
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities, involvement of the police.

My Agreement:

I agree to follow the safe practices and to support the safe and secure culture of IT use throughout the School.

Name ________________________________

Signed ________________________________

Date ________________________________

Click here to return to contents page