Castle Hill School
Innovating, Communicating, Empowering

Online Safety Policy

Policy Created: May 2014
Committee: LGB
Last review: October 2024
Review frequency: 1 Years
Date to be reviewed: October 2025

Contents

General Policy Statement

At Castle Hill School we intend to provide a safe, secure, caring environment where everyone is valued and respected equally. We aim to provide an inclusive education where children develop independent learning skills and are taught according to need, irrespective of their age, gender identification, sexuality, background, beliefs or abilities.

National legislation, the Equality Act 2010 and the Special Educational Needs and Disability Regulations 2014 re disabilities, race relations and special education needs underpin this policy, which has also taken into consideration national, local and school policies on Special Educational Needs, Equal Opportunities and Health and Safety.

General Curriculum Statement

The fundamental principle behind curriculum design at Castle Hill School is personalisation. The learning needs of each pupil are rigorously assessed on entry to the school and on a regular basis through their school career. This work has included a full audit of learning needs. In this, every aspect of each pupil's learning needs is reviewed, bringing in the experience and expertise of a wide range of staff, professionals and parents/carers to identify priority areas for the pupil's personalised curriculum. Each pupil's curriculum is therefore bespoke.

The ICT and Computing Curriculum at Castle Hill School enables students to develop digital literacy and computing skills to enable them to engage in cross curricular subjects and make positive contributions to the modern world and to be responsible and keep themselves safe online. Where appropriate, pupils will develop functional use of computing technology to enable them to communicate confidently and safely.

Philosophy

At Castle Hill School ICT and Computing is adapted for our students and predominantly serves a functional purpose alongside learning computing skills.

The use of computing technology is an integral part of the National Curriculum and is vital for everyday life. It is simply impossible to be a part of the modern world without a level of skill in the use of ICT and Computing technology; the students attending our school are 'Digital Natives' who have grown up in a world where they rely on, and are exposed to, ICT and computing from an early age.

At Castle Hill School, we recognise that learners are entitled to learn the skills needed to use appropriate technology effectively. Although they may have a user's familiarity with technology, the aim of ICT and Computing education is to give learners a deeper understanding of how a range of technology functions and enable them to programme, manipulate and create their own content at varying levels.

At Castle Hill School ICT and Computing is approached in a practical student centred manner tailored to our individual learners' needs. The study of ICT and Computing enables our students to expand their knowledge and understanding of the world by being actively involved in experiencing, investigating, manipulating and using information in a variety of forms including text, symbols, sound, graphics, photographs, music and video. For most of our learners, the core of ICT and Computing at Castle Hill School is communication, using a wide range of technology to engage with the world such as eye gaze, iPads and switches.

This policy applies to all adults, including volunteers, working in or on behalf of the school.

1. Aims

This Online Safety Policy recognises the commitment of our school to keeping staff and pupils safe online and acknowledges its part in the school's overall safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The Online Safety Policy supports this by identifying the risks and the steps we are taking to avoid them. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g., consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying;
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, contractors, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Expectations

This policy shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. We wish to ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken. We aim to minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

Our expectations for responsible and appropriate conduct are set out in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to online safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or inappropriate use.

3. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

- This policy complies with our funding agreement and articles of association.
  Online safety will be taught as part of the curriculum in an age-appropriate way to all pupils, where possible and appropriate.
- Online safety posters will be prominently displayed around the school.
- The Online Safety Policy will be made available to parents, carers and others via the school website or other online learning tools/apps

4. Roles and responsibilities

4.1 The local governing committee

The local governing committee has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The local governing committee will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The local governing committee will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The local governing committee will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing committee must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Til Wright.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with SEND
- To have an overview of how the school IT Infrastructure provides safe access to the internet and the steps the school takes to protect personal and sensitive data

4.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

4.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our safeguarding policy as well as relevant job descriptions. There are posters around school identifying the DSLs

The DSL takes lead responsibility for online safety in school, delegating to the ICT Manager where appropriate, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school safeguarding policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing board

This list is not intended to be exhaustive.

4.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

This list is not intended to be exhaustive.

4.5 All staff and volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Take responsibility for ensuring the safety of sensitive school data and information
- Maintain a professional level of conduct in their personal use of technology at all times
- Supervise pupils carefully when engaged in learning activities involving technology
- Ensuring that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all online safety incidents which occur in the appropriate log and / or to their line manager

This list is not intended to be exhaustive.

4.6 Parents and Carers (where possible and appropriate)

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- To agree and sign the child/parent use of internet which clearly sets out the use of photographic and video images of pupils
- support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

4.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

5. Educating pupils about online safety

(Where possible and appropriate)
We believe that the key to developing safe and responsible behaviours online for everyone within our school community lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We deliver a planned and progressive scheme of work to teach online safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. Online safety is taught in specific Computing and PSHE lessons and also embedded across the curriculum, with pupils being given regular opportunities to apply their skills.

We teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area. Staff and pupils will be reminded that third party content should always be appropriately attributed so as not to breach copyright laws.

We discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the AUP.

Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.
The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and pupils with SEND.

6. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, parent training sessions at school and in information via our website This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power (See also the school behaviour policy.)

7.2 Preventing and addressing cyber-bullying

For many of our cohort, their access to information technology and the internet is limited due to their cognitive understanding. For the minority of pupils who can access the internet independently, and use and understand social media interactions, we can support them through differentiated approaches. The following approaches are applicable to, and only appropriate for, this very small minority.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete the material, or
- Retain it as evidence (of a possible criminal offence* or a breach of school discipline), and/or
- Report it to the police**

* If a staff member **believes** a device **may** contain a nude or semi-nude image or an image that it's a criminal offence to possess, they will not view the image but will report this to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

** Staff will also confiscate the device to give to the police, if they have reasonable grounds to suspect that it contains evidence in relation to an offence.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Castle Hill School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Castle Hill School will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by Castle Hill School.

8. Acceptable use of the internet in school

All pupils, parents, staff, contractors, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

We provide the internet to

- Support teaching, learning and curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the school's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

9. Email

Email is regarded as an essential means of communication and the school provides relevant members of the school community with an email account for school based communication. Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. Email messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school email system is monitored and checked.

It is the personal responsibility of the email account holder to keep their password secure.

As part of the curriculum (where possible and appropriate) pupils are taught about safe and appropriate use of email.

Under no circumstances will staff contact pupils, parents or conduct any school business using a personal email addresses

Responsible use of personal web mail accounts on school systems is permitted outside teaching hours.

We will monitor the websites visited by pupils, staff, volunteers, contractors, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

10. Publishing content online

E.g. using the school website, learning platform, blogs, wikis, podcasts, social network sites

School website:

The school maintains editorial responsibility for any school initiated web site or publishing online to ensure that the content is accurate and the quality of presentation is maintained. The school maintains the integrity of the school web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

The point of contact on the web site is the school address, e-mail and telephone number. Contact details for staff published are school provided.
Identities of pupils are protected at all times. School obtains permission from parents for the use of unnamed pupils' photographs on the school website.
Group photographs do not have a name list attached.

Online material published outside the school:

Staff and pupils are encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school as they are in school.

Material published by parents, pupils, governors and staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

11. Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multimedia and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and video of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

We secure additional parental consent specifically for the publication of pupils' photographs in newspapers, which ensures that parents know they have given their consent for their child to be named in the newspaper and possibly on the website.

For their own protection staff or other visitors to school never use a personal device (mobile phone, digital camera or digital video recorder) to take photographs of pupils.

School will take photographs at whole school events; these will be made available to parents. This is due to keeping in line with the Safeguarding Policy and to ensure that pupils who do not have the appropriate publication permissions are kept safe.

12. Using video conferencing, web cameras and other online meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. We ensure that staff and pupils take part in these opportunities in a safe and responsible manner. All video conferencing activity is supervised by a suitable member of staff. Pupils do not operate video

conferencing equipment, answer calls or set up meetings without permission from the supervising member of staff.

Video conferencing equipment is switched off and secured when not in use and online meeting rooms are closed and logged off when not in use.

All participants are made aware if a video conference is to be recorded. Permission is sought if the material is to be published.

For their own protection a video conference or other online meeting between a member of staff and pupil(s) which takes place outside school or whilst the member of staff is alone is always conducted with the prior knowledge of the Principal or line manager and respective parents and carers. Please also refer to the to the ICAT Remote learning policy

13. Using mobile devices in school

We recognise that the multimedia and communication facilities provided by mobile devices (e.g. iPad, tablet, notebook, eye gaze device) can provide beneficial opportunities for pupils. However, their use in lesson time will be with permission from the teacher and within clearly defined boundaries.

Pupils are taught to use them responsibly.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

13.1 Using mobile phones - **Use of personal mobile phones is not permitted within the School.**

Where required for safety reasons in off-site activities, a school mobile phone is provided for staff for contact with pupils, parents or the school. Staff will never use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent. (*In an emergency, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.)*

Unauthorised or secret use of a mobile phone or other electronic device, including to record voice, pictures or video is forbidden. Publishing of such material on a web site which causes distress to the person(s) concerned will be considered a breach of school discipline, whether intentional or unintentional. The person responsible for the material will be expected to remove this immediately upon request.

The sending or forwarding of text messages, emails or other online communication deliberately targeting a person with the intention of causing them distress, 'cyberbullying', will be considered a disciplinary matter.

We make it clear to staff, pupils and parents that the Principal has the right to examine content on a mobile phone or other personal device to establish if a breach of discipline has occurred.

Trust(ICAT)/School owned mobile phones are permitted for use within office areas

13.2 Using wearable technology

Wearable technology includes electronic fitness trackers and internet enabled 'smart' watches.

Smart watches and Fitbits are permitted to be worn by staff but to be used only as a watch when working with children in keeping with professional responsibilities and expectations. Emergency

contact from external sources should be made via the school office rather than via mobile phones or other smart technology.

Personal devices are brought onto school premises by staff or pupils at their own risk. The school does not accept liability for loss or damage of personal devices.

Wearable technology is not to be worn during tests or examinations.

Unauthorised or secret use of a wearable device or other electronic device, including to record voice, pictures or video is forbidden.

13.3 Tracking devices

Tracking devices may only be brought into school with permission of the Principal.

13.4 Using other technologies

As a school we will keep abreast of new technologies and evaluate both the benefits for learning and teaching and also the risks from an online safety point of view.

We will regularly review the online safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

13.5 Use of Radios (Walkie Talkies)

- School radios (walkie talkies) communications are encrypted
- The language used whilst communicating on air should be professional and concise.

14. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Not tampering with the device encryption, all tablets/laptops leaving the school site are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Not tampering with the anti-virus / anti-spyware software

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT Manager

15. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

16. Managing and Safeguarding IT Systems

The school will ensure that access to the school IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for school activity.

All administrator or master passwords for school IT systems are kept secure and available to at least two members of staff e.g. Principal and member of technical support.

The wireless network is protected by a secure log on which prevents unauthorized access. New users can only be given access by named individuals e.g. a member of technical support.

We do not allow anyone except technical staff to download and install software onto the network.

16.1 Filtering

In order to be compliant with the Prevent Duty and Keeping Children Safe in Education, the school will:

- As part of the Prevent duty, carry out an annual assessment of the risk to pupils of exposure to extremist content in school
- Ensure that all reasonable precautions are taken to prevent access to illegal and extremist content. Web filtering of internet content is provided by a Smoothwall filtering appliance, Smoothwall; the provider is an IWF member and blocks access to illegal child abuse images and content. The provider filters the police assessed list of unlawful terrorist content produced on behalf of the home office. The school is satisfied that web filtering manages most inappropriate content including extremism, discrimination, substance abuse, pornography, piracy, copyright theft, self-harm and violence. However, it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own internet activity.
- Inform all users about the action they should take if inappropriate material is accessed or discovered on a computer. Deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

- Expect teachers to check websites they wish to use prior to lessons to assess the suitability of content.
- Post notices in classrooms and around school as a reminder of how to seek help.

16.2 Access to school systems

The school decides which users should and should not have internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

Staff are given appropriate guidance on managing access to laptops which are used both at home and school and in creating secure passwords.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to school systems is covered by specific agreements and is never allowed to unauthorised third party users.

16.3 Passwords

- We ensure that a secure and robust username and password convention exists for all system access (email, network access, school management information system). Multi Factor authentication is enabled for senior staff/finance staff/Teachers/Governors where possible to add an extra layer of security and protection.
- We provide all staff with a unique, individually-named user account and password for access to IT equipment, email and information systems available within school.
- All classes have a unique, individually-named user account and password for access to IT equipment and information systems available within school.
- All staff have responsibility for the security of their usernames and passwords and are informed that they must not allow other users to access the systems using their log on details. They must immediately report any suspicion or evidence that there has been a breach of security.

The school maintains a log of all accesses by users and of their activities while using the system in order to track any online safety incidents.

16.4 Protecting school data and information

School recognises the obligation to safeguard staff and pupils' sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The school is a registered Data Controller under the General Data Protection Regulations (GDPR) 2018 and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school will be controlled appropriately through technical and non-technical access controls.

Pupils are taught (where possible and appropriate) about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- Staff are provided with either an encrypted laptop or encrypted USB memory stick for carrying sensitive data offsite
- All computers or laptops holding sensitive information are set up with strong passwords, password protected screen savers and screens are locked when they are left unattended
- Staff are provided with appropriate levels of access to the school management information system holding pupil data. Passwords are not shared and administrator passwords are kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside school
- All devices taken off site, e.g. laptops, tablets, removable media or phones, are secured to protect sensitive and personal data and not left in cars or insecure locations.
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We follow Trust procedures for transmitting data securely and sensitive data is not sent via emailed unless encrypted/protected
    - Castle Hill School makes use of Microsoft Office365 for email and the use of the word 'secure' in the email subject will send the email using Office Message Encryption (OME). This ensures the email and attachment are delivered to the recipient in an encrypted method.
    - We refer to sensitive data as defined by the Information Commissioners Office (ICO) as personal data – Further explanation is available on their website (https://ico.org.uk)
- Remote access to computers is by authorised personnel only
- We have full back up and recovery procedures in place for school data
- Where sensitive staff or pupil data is shared with other people who have a right to see the information, for example governors or Kirklees officers, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies

17. Training

All new staff members will receive training, as part of their induction period, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety annually. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually through safeguarding training.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our safeguarding policy.

18. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the DSL and ICT Manager. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

19. Responding to online safety incidents

All online safety incidents are recorded in the School Online Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the DSL, their line manager or the Principal who will then respond in the most appropriate manner.

Instances of **online bullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's Online Safety Lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

19.1 Dealing with a Child Protection issue arising from the use of technology:

Please refer to our Safeguarding policy

20. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Prevent risk assessment
- TLT and Computing Policy
- TLT Code of Conduct (Local Governing Committee, Staff)
- TLT GDPR (Data protection) and privacy notices
- TLT Complaints procedure
- TLT Whistleblowing
- TLT Remote Learning
- TLT ICT and Internet Acceptable Use

Appendix 1: Parent/Child Use of Internet

Dear Parents/Carers

Responsible use of the Internet

At Castle Hill School we embrace technology and make use of ICT where possible and appropriate to enhance learning. Online safety is an important element in this process.

Our school Internet connection is provided by an accredited educational supplier and is filtered, which restricts access to inappropriate materials and is continually updating its database of known offensive sites. Access is also logged and monitored. Staff are also always present when pupils are accessing the internet.

As parents and carers, we also ask that you will support the school approach to online safety and not deliberately post comments or upload any images, sounds or text that could upset or offend any member of the school community or bring the school into disrepute.

To allow us to continue to offer internet access for learning please can we ask that you sign and return the slip below.

Yours sincerely,

Principal

✂----------

Pupil name……

I give permission for my child to use the Internet in School and will support the schools' approach to online safety.

Signed……(parent /carer)

Date……..

Please note: Permission remains active for length of time your child is at Castle Hill School.
Any changes to the above permissions need to be notified to us in writing.

Appendix 2: Acceptable Use Policy – Catering Staff
Castle Hill School Acceptable Use Policy Catering –School Cook
Responsible use of the internet, email and communication agreement

For the full policy governing the use of internet, email and electronic communications please refer to the Castle Hill School Online Safety policy, available in the policy folder on the server or hardcopy available upon request.

- all users of the schools IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,
- the school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited and e-mails exchanged
- users must not willingly make any changes to computer settings, delete any software or interfere with another person's work files
- permission must be obtained from the ICT Manager before any software is installed or downloaded from the Internet
- users are responsible for all e-mail sent and received, including from newsgroups, and will be vigilant about the risk of virus infection from files attached to e-mails
- 'Torrent' and 'Peer to Peer' file sharing is **prohibited** at all times
- laptops should **not** be used as **'home computers'** and should be used by the teacher/staff member only and not by other family members
- the same professional levels of language and content should be applied to e-mail as for letters or other media
- users will not use the Internet, email or mobile phones for personal use, personal financial gain, gambling, political purposes, social media (unless required for school use in their duty) or advertising (access to current affairs / education research at break times is permitted)
- copyright of materials must be respected
- use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is forbidden and may constitute a criminal offence
- accidental access to prohibited sites must be reported to a DSL/ ICT Manager/ SLT immediately
- **mobile phones must not be used in school with the exception of the Kirklees MBC supplied phone and tablet computer which are for work use only and will be only used within the kitchen**
  I will not use mobile phones, cameras or other electronic devices to take, publish or circulate pictures or videos of anyone without their permission
- I understand that I have an obligation to protect school data when working on a computer/laptop outside school and any school data must be stored on an encrypted device when being taken off site and will report immediately any accidental loss of confidential information so that appropriate action can be taken
- all online safety incidents are to be reported to on line safety officer / SLT immediately, which in turn will be logged. (Wherever possible the evidence should be preserved for inspection by the DSL/ICT Manager/SLT – i.e. if an inappropriate website is viewed, do not close the page but cover the screen / turn off monitor)

By signing this document you are accepting the terms of the Castle Hill on line safety policy, the above text is provided as a brief description of your responsibilities.

FULL NAME ……..

SIGNED …… DATE ……..

Appendix 3: Acceptable use agreement (staff, governors, contractors, volunteers and visitors)

Castle Hill School Acceptable Use Policy Staff, Contractors, Governors and Visitors

Responsible use of the internet, email and communication agreement

For the full policy governing the use of internet, email and electronic communications please refer to the Castle Hill School Online Safety policy, available in the policy folder on the server or hardcopy available upon request.

- all users of the schools IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently,
- the school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited and e-mails exchanged
- users must not willingly make any changes to computer settings, delete any software or interfere with another person's work files
- permission must be obtained from the ICT Manager before any software is installed or downloaded from the Internet
- users are responsible for all e-mail sent and received, including from newsgroups, and will be vigilant about the risk of virus infection from files attached to e-mails
- 'Torrent' and 'Peer to Peer' file sharing is **prohibited** at all times
- laptops should **not** be used as **'home computers'** and should be used by the teacher/staff member only and not by other family members
- the same professional levels of language and content should be applied to e-mail as for letters or other media
- users will not use the Internet, email or mobile phones for personal use, personal financial gain, gambling, political purposes, social media (unless required for school use in their duty) or advertising (access to current affairs / education research at break times is permitted)
- copyright of materials must be respected
- use of the network to knowingly access inappropriate materials such as pornographic, racist or offensive material is forbidden and may constitute a criminal offence
- accidental access to prohibited sites must be reported to the on-line safety lead / SLT immediately
- **mobile phones must not be used in school**
  (School mobile phones are available for use when taking pupils out of school).
- **I will not use mobile phones, cameras or other electronic devices to take, publish or circulate pictures or videos of anyone without their permission**
- I understand that I have an obligation to protect school data when working on a computer/laptop outside school and any school data must be stored on an encrypted device when being taken off site and will report immediately any accidental loss of confidential information so that appropriate action can be taken
- all online safety incidents are to be reported to DSL/ICT Manager/SLT immediately, which in turn will be logged. (Wherever possible the evidence should be preserved for inspection by the DSL/ICT Manager/SLT – i.e., if an inappropriate website is viewed, do not close the page but cover the screen / turn off monitor)

By signing this document, you are accepting the terms of the Castle Hill online safety policy, the above text is provided as a brief description of your responsibilities.

FULL NAME ……

SIGNED …… DATE ……

Appendix 4: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: Online safety incident report log

Online Safety Incident Report

Name of school: _____

This Event Report Form Compiled By: Name Title Date	
Staff informed: Name & Date	
Nature of Concern: Who was involved: pupil/staff/parents?	
Where did it occur: home, school?	
Time and date of Incident:	

Time and date the incident was logged:	
Action taken: (please tick) Evidence preserved Senior staff informed Other action	
Incident witnessed by: Staff Pupil Parent Other	
Other Officers Involved in Response: LA Officer LADO NCC Network Security Manager	

CEOP Police Other	
Follow up Action:	
Evidence Collected (and where retained):	
Review Date if required:	