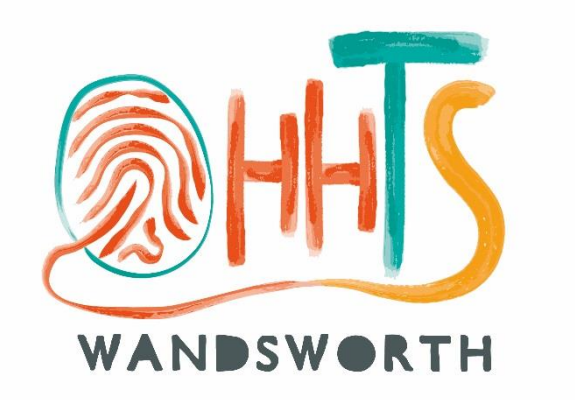


# ONLINE SAFETY POLICY

**Author:** Tara Bell
**Date:** 10th November 2022
**To be reviewed:** November 2023

**Approved by:** ……. **Date:** ……..

# Contents


- **Introduction**
- Aims
- Related Policies
- Legislation and Guidance
- Designated Safeguarding Leads
- School e-Safety: Strategies, Definition and Purpose of e-Safety
- Online Risks

- **Roles and Responsibilities**
- The Headteacher
- The E-Safety Officer
- Designated Safeguarding Leads
- The ICT Manager
- All Staff and Volunteers

- **Safeguarding**
- Pupils with Special Educational Needs and Disabilities
- Working with Parents and Carers
- Accessing and Monitoring the System
- Monitoring Computer Use

- **Teaching e-Safety**

- **Safe Teaching Practice**

- **Safe use of ICT, Internet and Search Engines**
- Chat Rooms and Instant Messaging
- Video Conferencing
- School Website
- Photographic and Video Images
- Mobile Phone and Handheld Systems

- **Responding to Incidents**
- Policy Statement
- Access to Inappropriate Websites
- Handling a 'Sexting'/Sexually Explicit Image Incident

- **Cyberbullying**

- Definition
- Forms of Cyberbullying
- Criminal Law
- Examining Electronic Devices
- Action by Service Providers
- Cyberbullying of Staff

- **Risk from Inappropriate contacts**

- **Risk from Extremism**

- **Training**

- **School Policy**

- **Other sources of Information and Support**

## Introduction

HHTS recognises that children and young people are growing up in a world dominated by information and communications technology (ICT) and the internet; both of which provide them with access to a wide range of information sources and increased opportunities for instant communication and social networking.

ICT is also an essential resource to support learning and teaching, but it can also present risks.

We also recognise that young people will continue to access the internet in other settings and localities. It is therefore HHTS' policy that the educational and social benefits of the internet and related technologies should be promoted in order to give our young people the skills to access life-long learning and employment, but that this should be balanced against the need to safeguard our learners. We wish to ensure that they are equipped and prepared to be safe users of the internet.

**Aims**

This policy document is drawn up to protect all parties including: the students; the staff and all members of the school community who have access to and are users of the service's ICT systems, both in and out of the school.

This policy aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements with respect to the use of ICT-based technologies.

HHTS aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**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 peer-to-peer 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

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

**This policy is to be read in conjunction with:**

- Safeguarding Policy
- Positive Behaviour Policy
- Whistleblowing Policy
- Disciplinary Policies
- GDPR Policy

**Legislation and guidance**

This policy is based on the Department for Education's (DfE's) 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
- [Relationships and sex education
- 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.

The policy also takes into account the National Curriculum computing programmes of study.

The **Designated Safeguarding Leads (DSLs)** are:

- Tara Bell - DSL
- Susan Arkley – Deputy DSL
- Anna D'Olier – Deputy DSL
- Megan Jones-Berney – Deputy DSL
- Hollie Oppe– Deputy DSL

The **e-Safety Officer** is Cameron Akitt

The **Safeguarding Lead,** and therefore e-Safety lead, for the Management Committee is Andy Hough.

**School e-Safety: Strategies, Definition and Purpose of e-Safety**

E-safety forms part of the "staying safe" element of the Government's *Every Child Matters* agenda, and all schools have a responsibility under the Children Act 2004 to safeguard and promote the

welfare of pupils, as well as owing a duty of care to children and their parents to provide a safe learning environment.

E-safety is a framework of policy, practice, education and technological support that ensures a safe e-learning environment in order to maximise the educational benefits of ICT whilst minimising the associated risks.

**Safe Systems:** Our Service is linked to the Internet via the London Grid for Learning (LGfL). We offer a safe e-learning environment by providing filtering to block access to unsuitable sites. In addition, all Service owned systems have up to date anti-virus software installed and can be monitored remotely by the School's ICT Manager and e-Safety Officer.

**Safe Practices:** The Service implements its policy and practice to ensure everyone is aware of the issues and knows what is expected of them in terms of their own acceptable use of the internet and other technologies. Our e-safety policy is consistent with related School policies such as Anti-Bullying and Behaviour.

**Online risks include:**

- Chat rooms and other social networking sites can pose a real risk to children as users can pretend to be someone else and take on an alias and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming"). Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. For example, home address details, telephone numbers, email addresses etc.
- The internet may also be used as a way of bullying a child, known as cyber bullying.
- Children are vulnerable to unregulated commercial activity (e.g. Phishing) on the Internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parents' credit card details, in response to offers for goods or services without seeing the fraudulent intent and realising the danger. Disclosing this type of information can lead to fraud or identity theft.
- Children can become involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
- Children may use information from the internet in a way that breaches copyright laws.
- Children may upload personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience and that material once published on the web is very difficult to remove.
- Children can be at risk of cyber-bullying
- Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment.

## Roles and Responsibilities

We understand that we have an important role in raising pupils' awareness of the potential dangers of using the Internet and helping them to develop their own strategies to avoid these risks and keep safe on-line.

Our strategy has the backing of the Management Committee, and is overseen by the Headteacher. As governing bodies have a statutory responsibility for pupil safety, it is vital that members of the Management Committee are aware of e-safety issues and support the Head and staff in the development of the Service's e-safety policy and strategy and help promote e-safety to all stakeholders.

The Headteacher has ultimate responsibility for e-safety issues within HHTS.

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board 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).

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 online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The headteacher

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

### 3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out above and in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, 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 child protection 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 headteacher and/or governing board

This list is not intended to be exhaustive.

**3.4 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 a weekly 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

This list is not intended to be exhaustive.

**3.5 The Role of ALL Staff and Volunteers:**

All staff, including contractors and 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 Service's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the behaviour policy
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- Ensuring that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA, through USO secure file exchange (USO FX) or Egress
- We require staff to use STRONG passwords
- We require staff to change their passwords every 90 days
- The Senior Leadership Team have a secure area on the network to store sensitive files

Teaching staff have a dual role concerning their own Internet use and providing guidance, support and supervision for pupils. Additionally, they are responsible for:

- Communicating the Service's e-Safety and Acceptable Use policies to pupils.
- Planning the use of the internet for lessons in advance, and researching on-line materials and resources.
- Reporting breaches of internet use to the Headteacher
- Recognising when pupils are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the Designated Safeguarding Leads and/or sharing key information through daily briefings, handovers and at clinical meetings.

**The Data Protection Officer's role includes:**

- Ensuring that all data controllers at the school handle and process data in accordance with data protection legislation.
- Ensuring that data in use remains up-to-date.
- Ensuring that data is destroyed in line with legal requirements when it falls outside of its retention period.
- Ensuring consent procedures meet the standards of the GDPR, identifying the data that requires consent
- Ensuring that, where a child is under the age of 16, parents have given consent on behalf of their child, unless the processing is related to preventative or counselling services offered directly to a child.
- Keeping comprehensive and accurate records of all data processing activities, detailing the purpose of the activity and making these records public upon request.
- Informing data subjects of how their data will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Undertaking audits of the school's data protection processes.
- Addressing any issues which are highlighted whilst auditing the school's processes.

## Safeguarding

Where any e-safety incident has serious implications for the child's safety or well-being, the matter will be referred to the Designated Safeguarding Leads who will decide whether or not a referral should be made to MASH in accordance with the Child Protection Policy.

**Pupils with Special Needs and Disabilities**

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

All staff are responsible for providing extra support for these pupils and should:

- Liaise with the e-Safety Officer and SENCo to discuss and agree whether the mainstream safeguarding systems on LGfL are adequate for pupils with this special need.
- Ensure that, in the case of Corner House pupils, the Acceptable Use Agreement is communicated to the pupil in their preferred language and ensure their understanding.
- Where necessary, liaise with the Service's ICT Manager to discuss any requirements for further safeguards to the internet or tailored resources and materials in order to meet the needs of pupils with SEND.
- Work with the e-Safety Officer to keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on pupils with SEND.

Staff should be aware that other children can also be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills, coupled with poor social skills and/or whose mental health predisposes them to make riskier choices.

**3.6 Working with Parents and Carers**

It is essential that parents and carers are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

Parents are provided with information on ICT and the School's e-Safety Policy as part of their welcome pack so that they are fully aware of their child's level of internet use within the school as well as the Service's expectations regarding behaviour.

Parents and carers of Home Tuition pupils are asked to sign a Home-School Agreement.

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

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

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

**3.7 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).

**Accessing and Monitoring the System**

Access to Service computers is via log-in and password.

The ICT Manager keeps a record of all log-ins used within the Service for the purposes of monitoring and auditing internet use and activity.

Where there have been prior concerns about internet use, recent incidents or issues raised via the MDT, students may have individual ICT plans such as limited use, no use within the classroom or use under 1:1 supervision.

All pupils sign an Acceptable Use Agreement in conjunction that sets out their rights and responsibilities and incorporates the Service's e-safety rules regarding internet use.

Staff sign an Acceptable Use Agreement on appointment and this is kept on record and updated annually.

**Monitoring Computer Use**

Staff carefully consider the location and position of computers in classrooms in order to allow an appropriate level of supervision of pupils depending on their age and experience.

Pupils may need to log-in to personal email accounts in order to access work from home schools; and may access sites such as YouTube for educational reasons. Staff need to ensure that they are closely monitoring students who are working independently.

## Teaching e-Safety

One of the key features of the Service's e-safety strategy is teaching pupils to protect themselves and behave responsibly while on-line.

Overall responsibility for the design and co-ordination of e-safety education lies with the Headteacher and Deputy Headteacher (Teaching and Learning), who is responsible for ensuring that all staff have the knowledge and resources to enable them to do so, but all teaching staff play a vital role in delivering e-safety messages.

**All** schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

The Computing Teacher/e-Safety Officer (in conjunction with the ICT Teaching Assistant at St. George's) is responsible for delivering content which covers:

- The benefits and risks of using the Internet
- How their behaviour can put themselves and others at risk
- What strategies they can use to keep themselves safe
- What to do if they are concerned about something they have seen or received via the Internet
- Who to contact to report concerns
- That the Service has a "no blame" ethos so that pupils are encouraged to report any e-safety incidents
- That the Service has a "no tolerance" policy regarding cyber bullying
- Behaviour that breaches acceptable use policies will be subject to sanctions and disciplinary action

- The School's network and access to the internet via the LGfL has been designed so that use is closely monitored and that access to inappropriate web sites is blocked and logged

In addition, pupils may be taught about evaluating and using internet content:

- As the internet is vast, pupils should be taught good research skills and how to critically evaluate the information retrieved. This can include questioning the validity of the source of the information; carrying out comparisons with alternative sources of information and considering whether the information is current and whether the facts stated are correct. In addition, pupils should be taught the importance of respecting copyright and avoiding plagiarism.
- Pupils should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.
- Pupils should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
- Social networking sites, groups and forums such as Facebook, Instagram and Twitter allow users, over 13 years, to publish information about themselves to be seen by anyone who has access to the site. Pupils are likely to use these sites out of school and need to be appraised of their dangers by an ongoing programme of information and advice.

These messages may also be delivered as part of other lessons, such as PSD, Safer Internet Day and wherever it would be appropriate to include curriculum wide.

Rules regarding the safe use of the internet are posted up in all classroom and teaching areas where computers are used to deliver lessons.

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

Students may be given access to the Service's Google Classroom, and are taught not to download and/or share content from their Google Classrooms externally.

**Content for explicit safety lessons will be taken from the appropriate key stage curriculum for each child.**

In **Key Stage 1**, pupils may be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** may be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils should know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, pupils may be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** may be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils should know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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 some pupils with SEND.

## 5. Educating parents about online safety

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

Online safety will also be covered during parent meetings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

## Safe Teaching Practice

All school staff need to be aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with pupils.

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

- Photos and video images of pupils are only to be taken by staff in connection with educational purposes e.g. school magazine/website
- Staff must ensure consent has been given for the use of any photos on social media, the website, within Service publicity materials and for any other public uses.
- Staff must always use Service equipment and only store images on Service computer systems
- Staff must take care regarding the content of, and access to, their own social networking sites and try to ensure that pupils and parents cannot gain access to these. All sensible precautions to ensure a private profile should be followed. Staff may well use Linkedin, on which they may list HHTS as a current employer. Young people have been known to use this site to seek information on teachers, and so the information made public should be carefully considered.
- Staff must ensure that any materials published on their own social networking sites are neither inappropriate nor illegal (please refer to job contracts and the Code of Conduct)
- Staff must be particularly careful regarding any comments to do with the Service or specific pupils that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.
- Staff should not engage in any conversation with pupils via instant messaging or social networking
- Where staff need to communicate with pupils regarding school work, this should be via their school LGFL account. Emails that are not directly related to their teaching or pastoral care, or are sent outside of school hours should be avoided as this may be misinterpreted or taken out of context. Staff members are also provided with an @hhts.co.uk email address through which to access Google Suite for Education.

- All emails and messages must be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.
- When making contact with parents or pupils by telephone, staff must only use Service equipment. Pupil or parent numbers must not be stored on a staff member's personal mobile phone and staff must avoid lending their mobile phones to pupils.
- Staff must ensure that personal data relating to pupils is always stored securely and encrypted if taken off School premises. No pupil identifiable data should ever be taken off site (e.g. first name/last name combinations, address and telephone numbers etc.)
- Where staff are using mobile equipment such as laptops provided by the Service, they must ensure that the equipment is kept safe and secure at all times and a user name and password combination is required to gain access.

## Safe use of ICT, Internet and Search Engines

- When using the internet, children must receive the appropriate level of supervision for their age, understanding and risk level. Staff should be aware that often, the most computer-literate children are the ones who are most at risk. Pupils should not be allowed to aimlessly "surf" the Internet and all use should have a clearly defined educational purpose.
- Despite strong filtering systems, it is still possible for pupils to inadvertently access unsuitable websites; to reduce risk, staff must plan the use of internet resources ahead of lessons by always checking the suitability of websites to be used.
- Where staff require access to blocked websites for educational purposes, this should be discussed and agreed with a member of the Senior Leadership team, who will liaise with the School's ICT Manager for temporary access.

All young people using social media for educational purposes, under our auspices, should be taught the correct use of privacy settings and how to keep safe on the internet. We must be aware that young people will use social networking sites outside of school, they should be advised:

- Not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended.
- Not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted.
- How to set up security and privacy settings on sites or block unwanted communications/ deny access to those unknown to them.
- To behave responsibly whilst on-line and keep communications polite.
- Not to respond to any hurtful or distressing messages but to let their parents/carer and/or teacher know so that appropriate action can be taken.
- Pupils should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the School's Anti-Bullying Policy.

### Chat Rooms and Instant Messaging

Chat rooms are Internet sites where users can join in "conversations" on-line; instant messaging allows instant communications between two people on-line. In most cases, pupils will use these at

home although the School might occasionally host these applications, under supervision, for specific educational purposes only.

Pupils should be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of School will not be tolerated and will be dealt with in accordance with the School's Anti-Bullying Policy.

**Video Conferencing**

Video conferencing enables users to communicate face-to-face via the Internet using web cameras. Video conferencing should only be carried out using LGFL approved School Based Solutions.

HHTS now has accounts with Google Meet, Zoom and Microsoft Teams. Teachers should avoid using other webcam sites on the internet due to the risk of inadvertent links to adult material.

Pupils' use of video conferencing should be for educational and or psychosocial purposes and should be supervised, as appropriate. When delivering home tuition remotely, a parent must be in the house, supervising.

Pupils must ask permission from a responsible member of staff before making or receiving a video conference call on Service owned systems.

Photographs and videos should only be downloaded onto secure (user name and password controlled) Service owned hardware and should never be associated with individual pupils' names or other identifying information.

*Please see Appendices for guidance on safe working remotely*

**School Website**

Content should not be uploaded onto the School website unless it has been authorised by a member of the Senior Leadership Team, who is responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

The Service has designated the e-Safety Officer and the School Administrative Officer as the named persons with responsibility for uploading materials onto the Service's website. The website will also be accessed and partially managed by Blue Apple.

To ensure the privacy and security of staff and pupils, the contact details on the website should be limited to the school addresses and the admin email and telephone number. No contact details for staff or pupils should be contained on the website. Children's full names should never be published on the website.

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

**Photographic and Video Images**

- Where the School uses photographs and videos of pupils online for publicity purposes, for example on the Service website, images should be carefully selected so that individual, named pupils cannot be identified.
- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers.
- Children's full names should never be published where their photograph or video is being used.
- Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

**Mobile Phone and Handheld Systems**

The majority of pupils are likely to have mobile phones or other equipment that allows them to access Internet services.

Use of mobile phones and handheld systems is not permitted during lessons. Mobile phones may be allowed on the wards; this is at the discretion of the Ward Manager and MDT.

Under no circumstances are children allowed to use their phones for taking photos of other children.

Mobile phones brought into school by staff members or visitors are entirely their own risk. The Service accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone and/or SIM card will be provided and used. 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.

## Responding to Incidents

**Responding to Incidents Policy Statement:**

All incidents and complaints relating to e-safety and unacceptable internet use will be reported to a member of the SLT in the first instance.

Where the incident or complaint relates to a member of staff, the matter must always be referred to the Headteacher for action.

Incidents involving the Headteacher should be reported to the Chair of the Board of Governors.

The School's e-Safety Officer keeps a log of all e-safety incidents and complaints and reviews the information for evidence of emerging patterns of individual behaviour or weaknesses in the Service's e-safety system, and uses these to update the e-Safety Policy.

E-Safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to a Designated Safeguarding Lead, who will make a decision as to whether or not to refer the matter to the Social Care Team.

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

**Access to Inappropriate Websites**

If a pupil or member of staff accidently opens a website that has content which is distressing or upsetting or inappropriate to the pupil/s' age, they should immediately (and calmly) close or minimise the screen. Staff should reassure pupils that they have done nothing wrong and discuss the incident with the class/pupil to reinforce the e-safety message and to demonstrate the Service's "no blame" approach.

The incident should be reported to a member of the SLT (and details of the website address and URL provided) who should liaise with the ICT Manager to ensure that access to the site is blocked and the filtering system reviewed to ensure it remains appropriate.

If a pupil deliberately accesses inappropriate or banned websites, they will be in breach of the Acceptable Use Policy and subject to appropriate sanctions. This should be reported to SLT as above.

If the materials viewed are illegal in nature the Headteacher should report this to the Chair of the Management Committee and/or the police and follow their advice, which should also be recorded on the e-safety incident report form. If deemed necessary, the ICT Manager can preserve evidence of websites which have been accessed on a particular device and/or identify which user accessed the materials.

**Handling a 'Sexting'/Sexually Explicit Image Incident:**

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish whether there is an immediate risk to a young person or young people

When assessing the risks, the following should be considered:

- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities?
- Does the young person understand consent?
- Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person - <u>In most cases, imagery should not be viewed</u>

- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult

2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)

3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent

4. The imagery involves sexual acts and any pupil in the imagery is under 13

5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police but in most cases a referral should be made to the MASH as there may be other information that the school are unaware of.

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and, if appropriate, local network of support.

## Cyberbullying

**Definition:**

The NSPCC (2018) define cyberbullying as follows:

> *Cyberbullying is an increasingly common form of bullying behaviour which happens on social networks, games and mobile phones. Cyberbullying can include spreading rumours about someone, or posting nasty or embarrassing messages, images or videos.*
>
> *Children may know who's bullying them online – it may be an extension of offline peer bullying - or they may be targeted by someone using a fake or anonymous account. It's easy to be anonymous online and this may increase the likelihood of engaging in bullying behaviour.*
>
> *Cyberbullying can happen at any time or anywhere - a child can be bullied when they are alone in their bedroom - so it can feel like there's no escape.*

Cyberbullying may take the form of:

- Rude, abusive or threatening messages via email or text
- Posting insulting, derogatory or defamatory statements on blogs or social networking sites
- Setting up websites that specifically target the victim
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or email (for example, “happy slapping”).

**Criminal Law**

In extreme cases, cyber bullying could be a criminal offence. There is not a specific law which makes cyber-bullying illegal but it can be considered a criminal offence under several acts, including:

- Protection from Harassment Act (1997)
- Malicious Communications Act (1988)
- Communications Act (2003)
- Obscene Publications Act (1959)
- Computer Misuse Act (1990)

The Service’s Anti-Bullying Policy, Positive Behaviour Policy and Acceptable Use Agreements cover the issue of cyber bullying and set out clear expectations of behaviour and sanctions for any breach.

Any incidents of cyber bullying should be reported to a member of the SLT who will record the incident and ensure that it is dealt with in line with the Anti-Bullying Policy. Incidents should be monitored and the information used to inform the development of future anti-bullying policies.

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

As part of e-safety awareness and education, pupils will be told of the “no tolerance” policy for cyber bullying and encouraged not to reply to offensive messages, but to report any incidents to school staff.

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/PSD) education, and other subjects where appropriate.

All staff, members of the Management Committee and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

**Action by Service Providers**

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

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

**Cyber Bullying of Staff**

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

The issue of cyber bullying of staff will be incorporated into any anti- bullying policies, education programme or discussion with pupils so that they aware of their own responsibilities. Incidents of cyber bullying involving staff should be recorded and monitored in the same manner as incidents involving pupils.

Staff should also be advised not to reply to any messages from pupils of a bullying nature.

**Risk from Inappropriate Contacts**

Staff may be concerned about a pupil being at risk as a consequence of their contact with an adult they have met over the internet. The pupil may report inappropriate contacts or staff may suspect that the pupil is being groomed.

All concerns around inappropriate contacts should be reported to the Designated Safeguarding Lead and safeguarding protocols and processes will be followed as per the Safeguarding Policy.

Where inappropriate contacts have taken place using Service ICT equipment or networks, the ICT Manager will ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other pupils is minimised.

**Risk from Extremism**

Many extremist groups who advocate violence use the internet as a means of either inciting hatred and violence or providing information on preparing explosives or carrying out terrorist acts.

Staff have all been trained in *Prevent*, and should be aware of potential influences and risks, and the action to take.

Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against School policies.

The Service should ensure that adequate filtering is in place and review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.

All incidents should be dealt with as a breach of the Acceptable Use Policies and the Service's Behaviour and staff disciplinary procedures should be used.

**Acceptable use of the internet in school**

All pupils, parents, staff, 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.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, 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.

**Pupils using mobile devices in school**

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Tutor group time
- Clubs before or after school, or any other activities organised by the school

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.

**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)
- Ensuring their hard drive is 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 locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

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.

**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 policies on ICT and internet acceptable use. 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 disciplinary procedures and staff code of conduct. 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.

**Training**

All new staff members will receive training, as part of their induction, 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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 child protection and safeguarding policy.

**Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. Staff should use normal safeguarding concerns forms on School Pod to report incidents.

This policy will be reviewed every year by the E-safety officer. At every review, the policy will be shared with the governing board. The review 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.

**School Policy**

Pupils and staff are expected to abide by the School's Acceptable Use Policy (AUP) at all times and use resources responsibly and safely. Where the AUP is breached and/or Internet use deemed inappropriate, the pupil/staff member will be subject to the provisions as stated in the AUP.

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department'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.

For further information, see the Wandsworth Safeguarding Board Online Safety Strategy http://www.wscb.org.uk/downloads/file/124/e-safety_strategy

This guidance is to be used in conjunction with Student and staff Acceptable Use agreements.

**Other Sources of Information and Support:**

http://www.wscb.org.uk/info/25/safety_online

https://www.thinkuknow.co.uk/

https://www.disrespectnobody.co.uk/

https://www.internetmatters.org/

https://www.saferinternet.org.uk/

https://www.childnet.com/resources/cyberbullying-guidance-for-schools

https://educateagainsthate.com/

https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

https://www.ceop.police.uk/safety-centre/

https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/

http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tacklingbullying

**Ofsted: Inspecting Online Safety**

http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-duringinspections-of-maintained-schools-and-academies

**Workplace bullying**

www.acas.org.uk

www.dignityatwork.org.uk

Appendix 1

**Acceptable Use Agreement: All Staff, Volunteers and Governors**

Covers use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, **equipment and systems.**

***Wandsworth Hospital and Home Tuition Service*** regularly reviews and updates all AUA documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the service's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Management Board.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, or any Local Authority (LA) system I have access to.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the service's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *LGfL StaffMail*
- I will only use the approved email system with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the headteacher.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will only use in staff areas or as deemed appropriate by the Headteacher.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff-only drive within the service.
- I will only I take or publish images of staff and students with their permission and in accordance with the service's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the service's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the LGfL / school approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Designated Safeguarding Lead if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Headteacher / Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.

- ***Staff that have a teaching role only****:* I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.
- I understand that I must comply with General Data Protection Regulations (GDPR) and the service's Data Protection Policy.
- I understand that any data breaches must be reported to the Service's Data Protection officer (DPO).
- I understand that if I wish to introduce or use any online IT systems or services that store or process pupil, parent or staff personal data I must liaise with the DPO in order for an audit and Data Protection Impact Assessment to be undertaken.

**Acceptable Use Policy (AUP): Agreement Form**

**All Staff, Volunteers, Management Board**

**User Signature**

- I understand and agree to abide by all the points above.
- I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the service's most recent online safety / safeguarding policies.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Signature .....Date.....

Full Name ..... (printed)

Job title / Role .....

**Authorised Signature (Head Teacher/ Deputy)**

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name ..... (printed)

## Photo Policy

HHTS Staff may use a digital camera to record classroom activities for displays, record keeping or publicity materials. These photos may be displayed within the hospital or in suitable environments outside the hospital including the HHTS website.

The photos may be stored on classroom computers for a short period of time before being deleted. It is your choice whether to have photos taken or not and you have the right to refuse at any tim

***I agree to have my photo taken and understand that it may be used in the hospital or outside the hospital for display purposes including HHTS website. I also understand that my photo may be stored on the classroom computers for a period of time.***

Signed: _____ Date: _____

## HHTS Agreement on Responsible Internet & ICT Use

**We have computers, iPads and Internet access to develop our learning. Whilst our Internet Service Provider has security software to prevent unacceptable material reaching us we cannot guarantee that all inappropriate content will be blocked. This agreement will help to keep everyone safe.**

- I will only use ICT in school for school purposes.
- I will only use the Internet with permission from a member of staff.
- I will ask permission from staff before I print.
- I will only access the network with the correct login and password.
- I will not access or try to access other users' files and materials on the network without their explicit permission.
- I will only email people with my teacher's approval.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I understand that teachers may check my computer files and may monitor the Internet sites I visit.
- I will not use or attach any storage device without a teacher's permission.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone I do not know in real life.
- I will support the service approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the service community.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

**If I do not respect this Agreement I understand that I will receive a temporary or permanent ban on Internet use.**

**Pupil name ……. Signature……**

**Date ……**

Appendix 3

| 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? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| 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 4**

## Guidelines for online lessons through Google Meet

HHTS offer additional tuition and support sessions to our students in receipt of home tuition though use of Google Education.

Students would need to sign into Google using their hhts.co.uk username and click onto Google Meet at the appointed time.

***HHTS teachers will:***

- Provide a timetable for students with appointments to 'meet' their teachers
- Teachers will be available at the agreed times, or let students/families know when 'meets' need to be cancelled or amended
- Offer on-screen tuition and support during these times

***Students will be expected to:***

- Join the online classroom at the agreed time, and inform staff in advance if they will not be available at the agreed time
- Be appropriately dressed and sat at a table in a designated part of the home
- Have resources sent by staff available
- Refrain from recording staff

Families/carers remain responsible for the students during these 'meets'. Staff will only have limited visibility of the students, and will not be responsible for their wellbeing.

**Appendix 5**

## Safeguarding measures in using Google Education

### Use of video teaching:

Staff need to protect themselves by ensuring that they take sensible precautions:

If you are delivering a lesson to a pupils at home, it is imperative that you check the parent is present in the same way that they would be present if you were visiting at home. You can ask this at the start of each tuition session and give parents advance warning that this will happen - like a little present/absent roll call for parents and student.

- Time of day – keep to school hours wherever possible. You will be given a timetable as to when you are expected to be online. Do not have video communications with students at any time outside of this timetable.
- Where is the pupil located during the session? – Ensure that CAMHS Campus School inpatient pupils are in the classroom or other appropriate ward room, supervised by a nurse or other clinician.
- Are they dressed appropriately?
- Is the parent aware this contact is happening / present?
- Ensure that you are dressed appropriately
- Ensure that no other people are in view (family/housemates) are in view whilst you are teaching.
- Ensure that the background is as plain as possible, and that there are no personal details or details which would reveal your home address etc., are in view whilst you are teaching.
- If you became aware that the lesson was being filmed or recorded, inform the pupil that this is unacceptable and end the videocall.

**Please inform SLT immediately if any of these guidelines are breached by pupils and families, or, even inadvertently, by yourselves.**

### Use of telephone contact:

- Telephone contact should only take place using HHTS phones – personal phones should not be used
- Wherever possible, talk to families and carers.
- If you need talk to the pupil, wherever possible this should be on a landline (if one is available) or via the parent's number
- If contact can only be via pupil's own phone – ensure you do not retain their number once the crisis has passed
- Record all direct contact; purpose and duration
- Ensure parental knowledge of contacts

### Use of remote working:

The Wandsworth Data Protection Officer advised that this is OK to remote in on our own devices/desktops, if we do not have a staff laptop, as long as we adhere to the Data Protection policy and the User Acceptance Agreement that we sign annually.

If you will be working on your own device, under all circumstances, please ensure that nothing is saved to your personal computer. Save back onto the network/Google Docs.

**Logging in remotely:**

**Username:** education\username ('education\initialsurname' – initialsurname is all lowercase, what we use to login to the network when we are onsite at Springfield)

**Password**: password (the usual password used to login to the network when we are onsite at Springfield)

**GENERAL SAFEGUARDING ISSUES:**

**Monitoring of vulnerable pupils**

- We will ensure that we remain in contact with all vulnerable and community pupils through weekly contact with them through Google Meet/Google Classrooms and through a check in call with families and carers. These contacts should be recorded on Schoolpod as lesson evaluations and onto our Safeguarding log for community students in Google education.
- All contact details are available through Schoolpod. Ensure any contact details are kept and used in line with GDPR regulations. The safeguarding log is then reviewed buy the community team, in house social worker and DSL's at the Tuesday community meeting. Any persistent absence is followed by a series of checks and actions as outlines in the community safeguarding guidance.

**Concerns:**

- If you have concerns relating to the safeguarding of pupils, please record in the normal manner – via Schoolpod.
- If a safeguarding concern is urgent, where you would normally hand the concern to a DSL in person, make contact with them via phone/email to ensure that they have seen it. We need to be mindful that staff may not be online at all times. If the DSL (Susan) cannot be reached, the deputy DSLs should be contacted (Tara, Anna, Megan). Do not assume that anyone has seen an email until you have had a response.
- Early Help Assessments can still be made through the MASH system: https://thrive.wandsworth.gov.uk/kb5/wandsworth/fsd/advice.page?id=QospX0VGq3c
- During this period, you may have additional concerns regarding COVID-19 outbreak related issues such as – inadequate food/supervision (neglect), young people acting as young carers and so on. Please follow normal safeguarding procedures.