



Hillcrest School Cramlington



Digital Safety Policy

Date established by Governing Body:	September 2020
Date for Full Implementation:	September 2020
Policy Ref No:	SP- Digital Safety Policy V2
Approved by:	Head Teacher Chair of Governors
Date:	27 January 2026
Review Frequency:	Yearly
Last Reviewed Date:	Rewritten from previous policy 19-20
Next Review due by:	January 2027

Contents

Introduction	3
Aims	3
Legislation and guidance	3
Responsibilities	3
E-safety Curriculum	5
Content	5
Expectations	5
Delivery	6
Resources	6
School Wide Focus	6
CPD	6
Bespoke support for specific circumstances	6
Family Support- online safety	7
Cyber-bullying, Prevent & Hate Crimes	7
Definition	7
Preventing and addressing cyber-bullying	7
Safety and Security	8
Examining electronic devices	8
Monitoring & Filtering	8
Acceptable use of the internet in school	8
Pupils using mobile devices in school	8
Publishing Information Online- School Website	8
Staff, Governors & Visitors	9
Staff using work devices outside school	9
How the school will respond to issues of misuse	9
Social Media & Professional Conduct Online	9
Training	9
Protocols	9
Incident Flowchart	10
Links with other policies	11
Appendix 1- AUP for Pupils	12
Appendix 2-AUP for Staff, Governors & Visitors	13
Appendix 3 Appendix- Online Teaching & Learning (inc. working from home)	15

Introduction

Hillcrest School works with a broad range of secondary learners with complex needs. Many of our students have access to the digital world through a variety of devices both within school and at home. We recognise both the value and the vulnerabilities this brings and as such will capture these in this policy along with appropriate measures to safeguard our young people. This policy will also share how we will support parents, carers and families in ensuring they can sufficiently safeguard their children at home.

This policy will also ensure staff have clear understanding of how they can keep themselves safe online and signpost them to training, support and guidance.

Aims

Our school aims to:

- Have robust processes in place to ensure the safety of pupils, staff, volunteers and governors when using digital devices
- Deliver an effective approach to online safety, which supports us in protecting and educating pupils, staff, volunteers and governors
- Establish clear mechanisms to monitor/identify, intervene and escalate an incident, where appropriate
- Develop confidence in becoming a positive digital citizen, including how to manage digital footprints and vulnerability online

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](#)
- [Relationships and sex education](#)
- [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.

The policy also takes into account the National Curriculum ICT programmes of study and OCR Digital Employability.

Responsibilities

Governing Body

The Governing Body has responsibility for adopting, developing and reviewing this policy and ensuring that effective monitoring systems and procedures are in place.

The Governing Board will have regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the e-safety lead.

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

Senior Leadership Team (SLT)

The SLT will:

- provide all staff with a copy of this policy and obtain receipt from each member of staff that s/he has read and understood the policy
- ensure that staff understand this policy, and that it is being implemented consistently throughout the school

The E-safety lead

The E-safety lead takes 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, Subrideo, Jeremy Neave and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with the agreed procedure
- Updating and delivering staff training on online safety
- 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.

Infrastructure Support

Northumberland County Council and Subrideo (Hardware/software technicians) are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure that software, network and hardware needs fall in line with GDPR and data protection requirements

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 school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- Working with the e-safety lead to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the agreed school procedure

This list is not intended to be exhaustive.

Parents and Carers

Parents are expected to:

- Notify a member of staff or the headteacher 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

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 factsheet - [Childnet International](#)

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.

E-safety Curriculum

Content

Pupils will be taught about online safety as part of the ICT & PSHE (inc. RSE, September 2020) curriculum and WJEC Pathways Qualifications for IT Users.

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see section 135 of KCSIE 2024).

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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.

These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other apps and sites.

As Hillcrest is a secondary specialist school, students will follow a phased curriculum. This is ensure any previous gaps in learning are covered but also to match the curriculum to their social, emotional and developmental needs.

iASEND S		iASEND E		iASEND N		iASEND D
Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6	Beyond
Safe image searching SMART rules for internet safety My personal information Email Making the right choice online	Digital footprints Searching 'keywords' Judging if websites are appropriate Rate and review websites Being kind online Safe and sensible online in different situations	Cyberbullying Buying online Creating safe passwords and changing privacy settings Safely send and receive emails Communicating online-safely	Cyberbullying Using search engines accurately Copyright and plagiarism Creating safe profiles- social media or game accounts Being a good digital citizen	Spam- what is it and how to recognise Writing citations for websites used Powerful passwords False photography Online safety stories	Cyberbullying Secure websites People online-relationships and information sharing Stereotypes online Evaluating my online activities	Digital Wellbeing Online Reputation Social Media Screen Time Online grooming Online relationships Adult content Prevent & Radicalisation

Expectations

By the end of Hillcrest school, pupils will 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
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not 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

Delivery

The content of the online safety sessions will often be taught as part of the ICT/PSHE programme of study and WJEC Entry Pathways Information and Communication Technology. It is likely these will be tailored to fit in within a theme but lessons may be isolated if linked with a topical or needs requirement. We also have a dedicated e-safety lesson per ½ term.

Resources

As technology is always evolving it is likely that many resources used will be online animations and videos. As part of the resource banks we use staff will also use photos, screen shots and activities from various trusted resource networks.

As online safety is a relatively practical subject we will use technology, programmes and the internet to further enrich the learning that takes place. We would not be asking students to bring in or use any of their own devices in school.

The school will also use resources provided by reputable companies- google, Barclays, School 360

School Wide Focus

Throughout the school year we have various events in where we promote digital safety. These are:

- Safer Internet Day
- Anti-bullying Week

CPD

CPD will be provided, throughout the year, for staff using accredited/registered organisations. The CPD will be around specific technologies, the curriculum content or resources to deliver the digital safety curriculum. Staff can source their own CPD using recognised providers such as:

- Childnet
- Internet Matters
- SWGfl (South West Grid for learning)
- NSPCC
- CEOP
- Think u Know

Specific CPD for staff:

- Safer working - LADO
- Safer school culture training - HR
- E-safety training – Annual Online Refresher Training - NCC

Bespoke support for specific circumstances

Due to the nature of our setting it may be that students require specific support, guidance and education around their own circumstances. This may be taught within class or delivered by the Student Support Team. Example interventions could be:

- Dealing with cyber bullying
- Managing online relationships
- Healthy internet interests
- Managing screen time
- Gaming addictions
- Sexting and getting nude online
- Online communities- chatting

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Family Support- 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. Examples of communication home:

- 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.

Monitoring & Filtering

The internet content and access is filtered through Lightspeed. The content controls are managed by Northumberland County Council e-safety team.

Within school we monitor usage and content through SensoCloud. This is an intelligent monitoring software which monitors all devices within school. Any potential violations are then captured through a screen shot. Each Monday a report is sent through to the DSL and E-safety lead. Each capture will need checked and categorized depending on the content. In addition, specific keywords are flagged through SensoCloud and the Headteacher/Deputy Headteacher and informed via email to enable them to respond in real time.

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 1-3). 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, 2 and 3.

Pupils using mobile devices in school

Pupils may bring mobile devices into school with the intention of them being used for their safety on their journey to and from school. They are not permitted to use these at any point whilst on site. The procedures for mobile phones onsite are:

- Pupil switches off mobile device before entering school site
- Mobile device is safely stored until the end of the school day, pupils can turn these on once they are off the school site
- If a pupil refuses to follow these arrangements a call will be made for parent/carers to collect the device

Publishing Information Online- School Website

Hillcrest will use the website as a primary means of communication with parents/carers and the wider community. The information posted will always be authorised by the Headteacher before being posted online. No information will be shared that will identify a pupil or pictures posted unless prior authorisation has been given.

Staff, Governors & Visitors

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from Subrideo, Jeremy Neave or SLT.

Work devices must be used solely for work activities.

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 the flowchart. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The Headteacher and Deputy Headteacher receive weekly reports from SensoCloud and Lightspeed and will follow up any reported incidents.

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 & 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 or LADO (Local Authority Designated Officer).

Social Media & Professional Conduct Online

Northumberland County Council provide a policy for staff 'Social Networking Policy' which has been adopted by the governors of Hillcrest. Alongside our 'Code of Conduct', 'Staff Handbook' and 'Hillcrest Expects...for staff' documents there is clear guidance given to staff about keeping themselves safe and preventing the reputation of the school coming into question. Some of the key aspects covered in the Social Networking policy are:

- Clear distinction between personal and business use of social media
- Caution over posting or sharing and personal information that may bring the school into disrepute
- It is the users responsibility to protect their own professionalism
- No contact should be made with pupils

Link for professionals online safety helpline: <https://swgfl.org.uk/services/professionals-online-safety-helpline/>

Training

All new staff members will receive information, support and guidance 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).

The DSL and 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.

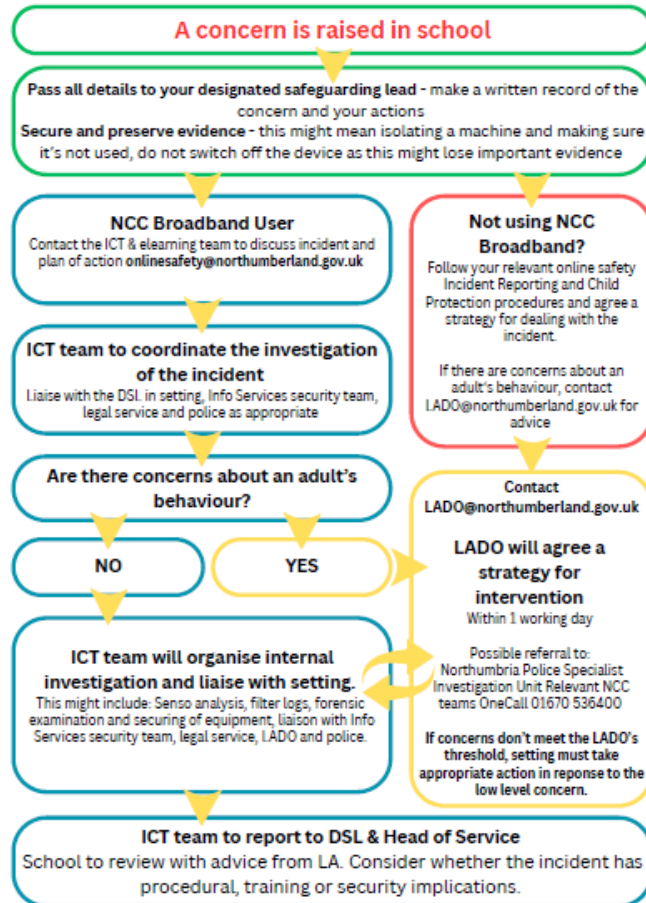
Protocols

The DSL logs behaviour and safeguarding issues related to online safety using our CPOMs safeguarding platform.

Incident Flowchart

The following incident flow chart is produced by Northumberland County Council e-safety team.

Reporting an online safety incident - all settings



Links with other policies









This online safety policy is linked to our:

- Child protection and safeguarding policy
- Relationship policy (formerly behaviour policy)
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Social Networking Policy
- Hillcrest expects....for staff
- Anti-bullying Policy

Appendix 1- AUP for Pupils

Acceptable Use Policy for Pupils

To keep everyone safe when using computer equipment at school I will:

- hand my mobile in when I arrive at school. I will get it back at the end of the day. 
- use the computers safely at all times.  
- understand that I am responsible for my own actions. I know that school software checks computer files and monitors what sites I use.
- not use other people's accounts or files.
- only use programs that are already on the school computer or I-Pad.
- report any inappropriate material messages to staff. I know I can click the CEOP button to report inappropriate material. 
- only take appropriate photographs or videos using school equipment. I will ask for permission. 
- only send e-mails with permission from my teacher. 
- remember not to share my personal information. For example, full name and address.
- not access social networks or chat rooms. 
- Remember to treat others fairly and not upset people online. 

Name of Pupil: _____

Class: _____

Signed by Pupil: _____

Date: _____

Appendix 2-AUP for Staff, Governors & Visitors

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of all technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Appendix 3 Appendix- Online Teaching & Learning (inc. working from home)

As part of extending the curriculum offer, Hillcrest school will provide access to e-learning resources. These will enhance or extend the learning that is taking place in the classroom. The learning will be through education APPs, online links, SeeSaw or using the School360 platform, which includes the use of emails.

No other platforms, means of communication or social media should ever be used for contact with students, parents or carers.

Online Learning platforms and APPs

All learning platforms and APPs will be managed by Hillcrest school, so that the certification and robust data protection policies can be followed. It is also important that a member of the SLT would remain an admin on all platforms and APP based learning resources.

Staff working from home

Staff working at home can choose to use their own devices, if they are confidently able to safeguard the information and use of these. If staff do not have access to online devices Hillcrest school will support, where possible, so this is not a barrier to working from home.

Some key information for staff working at home:

- It is essential that all usernames, passwords and log on information is easily accessible
- Any digital files required at home should be emailed or held temporarily on googledrive so they can be uploaded back onto the secure network once back in school. **Any items viewed/downloaded should be deleted from staffs' devices and removed from the bin.**
- No other users at home should view, be able to access or communicate school information, including information about pupils, staff and documentation
- If staff are not confident in the use of devices at home they should seek further advice
- Staff should not use any methods that have not been previously agreed by the headteacher to complete work, transfer information or contact students/colleagues
- Staff should take care of their own mental and physical health whilst working from home

Any safeguarding concerns, must be shared with the DSL and use appropriate routes to share these concerns: phone call and CPOMs.

DOCUMENT HISTORY – VERSION CONTROL

Item	Change	Date of Update	Document Version
Whole Policy	Overall, review of policy- no changes.	Sept 2020	SP- Digital Safety v2
Whole Policy	Reviewed Policy -		

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided ([amend/delete as relevant](#)) through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day_and Anti-bullying week_

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to ([insert relevant person](#)) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies ([n.b. the guidance contained in the SWGfL Safe Remote Learning Resource](#))
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Online Safety Education Programme

[While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.](#)

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum ..."

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- *learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the CyberChoices site.*
- *staff should act as good role models in their use of digital technologies the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- *where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit*
- *it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need*
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Document History

Item	Nature of Change	Date of Update	Document Version
Digital Safety	Document history added Policy References updated	16/05/2025	Digital Safety v4