THE HALL SCHOOL

Online Safety Policy

AUTHOR: Jess Johnson / Katie Bonham Carter

Policy ratified by: SLT

Date of publication: September 2021

Date of next review: September 2022

Governor responsible for policy: Victoria Bingham

This policy is available on the School website and can be made available in large print or other accessible format if required.

Online Safety Policy

1. Managing the Internet Safely

1.1 Introduction

The educational and social benefits for children in using the internet should be promoted, but this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, schools need to be able to teach children how to keep themselves safe whilst on-line.

This document provides guidance on developing an effective online safety strategy so that these aims are achieved and to support staff to recognise the risks and take action to help children use the internet safely and responsibly.

1.2 Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking. As use of technology is now universal, children need to learn computing skills in order to prepare themselves for the working environment and it is important that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

1.2.1 Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

1.2.2 Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names 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") with a view to sexually abusing them.

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.

The internet may also be used as a way of bullying a child, known as online bullying. More details on this can be found in section 4.5 of this policy.

1.2.3 Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

1.2.4 Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

· becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people

· using information from the internet in a way that breaches copyright laws

· uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience

· online bullying (see section 4.5 for further details)

· use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

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. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

School online safety strategies

2.1 Purpose and description

Computing is now a key part of the school curriculum and one of the key aims of computing is to ensure that pupils are aware of online safety messages. This is part of the Hall school's responsibility to safeguard and promote the welfare of pupils, as well as the duty of care to children and their parents to provide a safe learning environment. It is recognised that abuse can take place wholly online or technology may be used to facilitate offline abuse.

The Hall has an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

· promote the use of technology within the curriculum

· protect children from harm

· safeguard staff in their contact with pupils and their own use of the internet

· ensure the school fulfils its duty of care to pupils

· provide clear expectations for staff and pupils on acceptable use of the internet.

In particular, The Hall:

- Maintains broadband connectivity;
- Maintains the system to ensure that it remains robust and protects students;
- Has additional user-level URL filtering in place using the Lightspeed;
- Ensures network health through appropriate anti-virus software Sophos and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs;
- Utilises caching as part of the network set-up;
- Ensures the network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows pupils access to Internet logs;
- Class log-ins are used to access the school network for pupils;
- Individual school log-ins are used for all staff users;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured; Never allows personal level data off-site unless it is on an encrypted device;
- Encourages 'safer' search engines with pupils such as | hhttp://primaryschoolict.com/ and activates 'safe' search modes where appropriate;
- Ensures pupils only publish within appropriately secure learning environments such as Office 365 or Firefly.

2.2 Teaching and Learning using the internet:

This school:

- Supervises pupils' use at all times, as far as is reasonable, when children are using computer equipment;
- Uses the Lightspeed filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Ensures all sites are previewed by staff before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines (such as Yahooligans, Ask Jeeves) where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing Co-ordinator and Computing Technician.
- Only uses Office 365 for pupil's own online creative areas such as web space and ePortfolio;
- Only allows pupils to use Office 365 or approved Learning Platform discussion forums/threads in school.
- Only uses approved or checked webcam sites;
- Only allows pupils to download music clips from sites approved for educational purposes where there are no copyright or legal implications;
- Requires pupils (and their parent/carer) to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an online safety / acceptable use agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures a named DSL has appropriate training
- Ensures parents provide consent for pupils to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their son's entry to the school;
- Makes information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities.

2.3 E-Safety and Internet Use Education Programme

This school:

- Fosters a 'No Blame' environment that encourages pupils to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures pupils and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or technician;
- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Has a clear, progressive e-safety education programme throughout all year groups, built on national and Becta guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to expect a wider range of content on the internet, both in level and in audience, than is found in the school library or on television;
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
    - to not download any files – such as music files - without permission;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
    - to have strategies for dealing with receipt of inappropriate materials.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include, risks in pop-ups; cyberbullying; online gaming / gambling.
- Provides advice, guidance and training for parents, including:

    - Information in safety leaflets and on the school web site and Firefly learning platform;
    - suggestions for safe Internet use at home;
    - Availability of 'Think U Know' for parents on the Firefly learning platform;
    - provision of information about national support sites for parents;

- Online Safety evening to be held annually for all parents.

3.Managing Email

3.1 This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example j.bloggs@hallschool.co.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.

- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Manages accounts effectively with up to date account details of users.
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of services to help protect users and systems in the school, including desktop anti-virus product and spam filtering.

3.2 Pupils:

- Boys at the start of Year 4 have access to their own email accounts
- Boys are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
    - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.

3.3 Staff:

- Staff can only use their school mail systems on the school system.
- Staff only use their Hall School e-mail systems for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed.
- All staff to sign that they have read and understood the contents of this policy.

3.4 How emails will be managed:

Regulated email is filtered and accountable. Use may also be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence. The school hall has appropriate educational, filtered Internet-based e-mail options.

- If a serious safeguarding issue arises concerning the use of email, the procedure outlined in the Safeguarding Policy will be put in place.

3.5 Procedures:

- The use of personal e-mail addresses for professional purposes, such as Hotmail, must be avoided by all staff working in schools. Staff are required to use the appropriate Hall School email for professional purposes.

- Many teenagers will have their own e-mail accounts, such as the web-based Hotmail or G-mail, which they use widely outside school, usually for social purposes. These should not be used for school purposes. Where e-mail accounts are not monitored, there is the risk that pupils could send or receive inappropriate material. External web-based e-mail accounts with anonymous names such as pjb354@emailhost.com make monitoring and tracing very difficult and require support from the providers of the email system (who may be an international company).

- Personal email must not be used by staff to transfer information about pupils

3.6 Education:

- Staff and pupils are made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the school's Online Safety and anti-bullying education programme.

4. Using digital images and video safely

4.1 In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website and VLE content is accurate and quality of presentation is maintained;
- The school web site complies with the school's guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Pupils are made aware of copyright issues when updating parts of the school website and are taught to source images from copyright free sources or credit the sources used.
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Staff are made aware that photographs/digital videos of pupils may only be used if parental permission for this has been gained. Class teachers are given a list of pupils with photography permission at the beginning of each school year;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication. At the end of the year, photographs and digital videos are archived onto CD and kept in a locked storage room;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Pupils are only able to publish to their own 'safe' web-portal in school;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are taught about how images can be abused in their Online Safety education programme;
- The school will block / filter access to inappropriate social networking sites;
- Pupils will be advised never to give out personal information of any kind which may identify them and / or their location. Examples would include real-name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends, specific interests and clubs etc;
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding the background detail in a photograph which could identify the student or his / her location e.g. house number, street name or school (notify staff of this change);
- Pupils should be advised on security and encouraged to set passwords and deny access to unknown individuals. Students should be encouraged to invite known friends only and deny access to others;

- Students should be advised not to publish specific and detailed private thoughts;
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comment.

5.Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- All pupils have their own unique username and password which gives them access to the Internet and the VLE;
- Makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Staff are responsible for ensuring that doors to the ICT suite are closed (including fire exits) after lessons. At the end of the school day, staff are responsible for shutting down all consoles;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- We request that they DO switch the computers off at the end of the day;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that

they notify the school of any "significant personal use" as defined by HM Revenue & Customs;

- Maintains equipment to ensure Health and Safety is followed;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school;
  e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAS system;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO username and password);
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards.

Remote Learning

1**. Aims**

- The remote learning policy for staff aims to:
- Ensure consistency in the approach to remote learning for pupils who aren't in school
- Set out expectations for all members of the school community with regards to remote learning
- Provide appropriate guidelines for data protection

2. **Roles and responsibilities**

Should we have to return to a period of online teaching, we will continue with the normal timetable in the JS and MS/SS.
Please be aware of the following guidelines/expectations:

2.1 Teachers

When providing remote learning, teachers must be available between 8.00am and 4.00pm and any relevant meetings outside of this time, unless otherwise specified in your contract.

Absence during remote learning

If you are unable to work for any reason during this time, for example due to sickness or caring for a dependent, you should report this using the normal absence procedure (contact line manager and WS or KBC by 7.15am).

Absence due to COVID test/asymptomatic during school opening

If you are either awaiting the result of a COVID-19 test, or if you are asymptomatic and able to teach you should adhere to the teaching expectations below:

- You should notify your line manager/relevant member of SLT (WS/KBC) of your absence before 7.15am and if possible, how long it will be for.
- A cover teacher will be allocated to your class as normal, however they will only be there to monitor the class.
- You should make use of Microsoft Teams/Firefly/SeeSaw and GoToMeeting to run your lessons remotely at the relevant times. You should provide the relevant link to the cover teacher, so they can notify students on where to access the work and lesson.
- Students will be prompted by the cover teacher to join the online lesson and they will be able to assist the class if there are any issues.

Should you be unwell, you of course would not be expected to teach and should provide written cover as normal or ask you HoD/HoY to, if you are unable to.

Teacher responsibilities

When providing remote learning, teachers are responsible for:

Interactivity

- Each class in the MS/SS should already have be set up on Microsoft Teams and students made aware of this. It is ideal if Teams can be used from time to time in school to keep the students familiar with the platform
- Staff in the SS should continue to set prep using the online planner on Firefly- a link can be added to Teams.
- GoToMeeting or Teams should be used for all live video lessons, unless another platform has been agreed with AC/CG.
- Staff should ensure a degree of interactivity in their remote teaching, this does not mean your whole lesson has to be a live video, however a short live introduction using GotoMeeting or a short closing session accompanied by a narrated PowerPoint would be ideal, if you are unable to/it is not appropriate to broadcast the whole lesson. Additionally, making use of the posts section on Teams will also facilitate a dialogue with students when you are not able to be live on video. Please refer to the Teams guide and The Hall School Staff Guide to interactive learning for further guidance.
- Any technical-related or digital learning issues please use techsupport@hallschool.co.uk during periods of remote learning only.

Setting work for students/quality of instructions

- Please ensure you provide work for each class you teach and the number of lessons they have each week.

- Prep may be set, however if the task can be based offline this would be preferable to reduce screen time. Please refer to the prep policy for details on how much for each year group.
- Please ensure you are providing clear instructions to the students that they can act on themselves and require minimal or no parental input.
- In the Middle and Senior school staff should use Microsoft Teams to set tasks for their classes accompanied by a GoToMeeting where possible. So, each subject class and form group should have their own team. Firefly can also be used to set tasks, but a notification should be placed on Teams. We should, however, be mindful that pupils' and students' (and our!) broadband speeds may not be adequate to participate fully in interactive teaching online. If it is clear that one participant is not able to keep up, the provision of the lesson should change to a less interactive mode for that student. Likewise, we must recognise that home filters may block different content from school filters, and we should ensure that if content is blocked from a user, an alternative is suggested.
- Staff in the JS should use SeeSaw and GoToMeeting where suitable.
- Unless requested otherwise work should be set on the day of the lesson
- If school is open and a student is too unwell to attend school with a non COVID illness (e.g. cold, sickness etc) they should not be provided with work as they should be resting and recuperating at home and should catch up once they have returned.
- Should a student be isolating at home for a prolonged period due to a positive COVID test, but are well, then work should be provided by their teacher. If the student is unwell, they should not be expected to complete work until they are better. In the MS/SS each teacher should use Microsoft Teams to share the work with the student, as this will reduce the number of emails being sent with attachments. Firefly should still be used for prep setting and the student should regularly check their online planner for prep. In the JS work should be provided via SeeSaw, or paper copies if applicable.

Feedback

Where possible please ensure you are providing timely and appropriate feedback to your students, following the feedback and marking policy where feasible and appropriate. This also includes when using online programmes. Feedback may be verbally given, written in an email, by hand and a scanned copy sent via email, or directly on a shared document by the comments feature.

Flexibility

Whilst we will need to set deadlines for tasks, please be flexible with this and when chasing students for work.

Keeping in touch with pupils who aren't in school and their parents

- Form tutors are expected to be in contact with their form each morning during form time using GoToMeeting
- Teaching staff are expected to be in contact with their classes during each timetabled lesson.
- Staff should respond to student and parent emails in a timely manner, this should be within 24 hours even if a holding email is only sent.
- Staff are not expected to respond to emails outside of working hours or at weekends.

- Staff should only communicate with parents and students via school email, Microsoft teams, GoToMeetings or School Cloud for parents evening, or Zoom if prior agreement has been given by AC/CG.
- Staff should where possible, deal with complaints in the first instance themselves, however depending on the nature of the complaint these may need to referred to line managers and/or SLT or DSL. Formal complaints will be dealt with via the formal complaints procedure (see Complaints policy).
- In the first instance staff should deal with behavioural issues themselves where suitable, this may be emailing parents, talking to a Form Tutor about the issue etc. In some cases some issues may need to be passed up to Heads of Year/Head of Department/SLT who will make contact with parents.

Attending virtual meetings with staff, parents and pupils

- GoToMeeting should be used when holding meeting with parents or students. Parents' Evenings will be held online using the School Cloud system.
- Dress code- when staff are on a video meeting they should be dressed smart casually
- Locations (e.g. avoid areas with background noise, nothing inappropriate in the background)

2.2 Teaching assistants

When assisting with remote learning, teaching assistants must be available between 8.00am-4.00pm and any relevant meetings outside of this time, unless otherwise specified in your contract.

If you are unable to work for any reason during this time, for example due to sickness or caring for a dependent, you should report this using the normal absence procedure (line manager and WS or KBC by 7.15am)

When assisting with remote learning, teaching assistants are responsible for:

Supporting pupils who aren't in school with learning remotely

- Supporting students on the learning support list and any other students who are identified as needing additional support
- Support should be provided remotely by either Microsoft Teams, GoToMeeting or Zoom (only with prior agreement from CG/AC)

Attending virtual meetings with teachers, parents and pupils – cover details like:

- GoToMeeting should be used when holding meeting with parents or students. Parents' Evenings will be held online using the School Cloud systems.
- Dress code- when staff are on a video meeting they should be dressed smart casually
- Locations (e.g. avoid areas with background noise, nothing inappropriate in the background)

2.3 Heads of Department/ JS Year Heads

Alongside their teaching responsibilities, subject leads are responsible for:

- Considering whether any aspects of the subject curriculum need to change to accommodate remote learning
- Working with teachers teaching their subject remotely to make sure all work set is appropriate and consistent
- Working with other subject leads and senior leaders to make sure work set remotely across all subjects is appropriate and consistent, and deadlines are being set an appropriate distance away from each other
- Monitoring the remote work set by teachers in their subject – (Weekly departmental meetings, reviewing work set, sharing examples of work)
- Alerting teachers to resources they can use to teach their subject remotely

JS Year Heads as above and,

- Have oversight of the curriculum being delivered across the year group and ensure that work is responded to appropriately.
- Liaise with the Specialist teachers to make sure they know when to deliver lessons and any changes to the week.

2.4 Senior leaders

Alongside any teaching responsibilities, senior leaders are responsible for:

- Co-ordinating the remote learning approach across the school
- Monitoring the effectiveness of remote learning – (teacher feedback, meetings (HoDs, SLT, MS/SS, JS, whole school meetings, regularly reviewing the RL policy, feedback from students, parents).
- Monitoring the security of remote learning systems, including data protection and safeguarding considerations

2.5 IT staff

IT staff are responsible for:

- Fixing issues with systems used to set and collect work
- Helping staff and students/parents with any technical issues they're experiencing
- Reviewing the security of remote learning systems and flagging any data protection breaches to the data protection officer
- Assisting pupils and parents with accessing the internet or devices

2.6 Pupils and parents

Staff can expect pupils learning remotely to:

- Be contactable during the school day – although consider they may not always be in front of a device the entire time
- Complete work to the deadline set by teachers

- Seek help if they need it, from teachers or teaching assistants
- Alert teachers if they're not able to complete work

Staff can expect parents with children learning remotely to:

- Make the school aware if their child is sick or otherwise can't complete work
- Seek help from the school if they need it
- Be respectful when making any complaints or concerns known to staff

All students/parents have signed and returned the contract below:

Remote Learning Contract for Parents and Pupils

In light of current circumstances, whilst school is suspended, our current approach to learning and teaching is through a range of online learning platforms and applications. These platforms are where our pupils access the curriculum through videos, assignments, question and answer streams and can also upload their work and receive feedback.

We would like to receive your permission for your son to participate in interactive learning. There are clear rules and parameters to which all pupils are expected to adhere.

To facilitate interactive learning during this time, parents are requested to help by:

- Providing their son with a workspace that is quiet, safe and free from distractions (not a bedroom) with an adult nearby if necessary
- Making sure that your son is dressed appropriately
- Ensuring that if there is face to face communication it is only between the teacher and the pupils.
- Ensuring that any parent to teacher communication is through the usual manner via email.
- Not recording, sharing or commenting on public forums about individual teachers.
- Interacting patiently and respectfully with teachers. Please be mindful of the fact that this is a new situation for teachers as well as pupils.
- To facilitate interactive learning during this time, pupils are requested to help by:
- Only using technology at home with the permission of your parent / guardian.
- Not revealing your password to anyone.
- Being responsible for your behaviour and actions when using technology, including resources accessed and the language used. Appropriate behaviour is expected in live sessions at all times. Inappropriate behaviour (e.g. posting inappropriate comments or images) will be managed in line with the school's Behaviour Policy.
- Ensuring that all of your communication with other boys and teachers using technology is responsible and sensible. The potential for getting into difficulties as a result of your online activities may increase as you have more of this time on your hands. Please remember - don't become 'friends' and don't allow 'followers' unless you know the person in real life.
- Behaving appropriately. Unkindness toward peers and bullying will not be tolerated. If you witness this, please report it. Don't be a bystander. We all have to work together to ensure that our community is behaving well toward each other.

- Completing and uploading all prep or class learning by the deadlines directed by the teacher.
- Not deliberately browsing, downloading, uploading or forwarding material that could be considered offensive or illegal. If you accidentally come across any such material you should report it immediately to your teacher or parent/guardian.
- Not recording or taking photos of classmates or teachers during video conferencing sessions, nor sharing lessons publicly.
- Noting and understanding that Microsoft Teams and other applications provided by the school record the lessons and their content, so an individual's use can be monitored and logged.
- Not initiating at any time 'Meet Now' in Teams.

Some teachers may incorporate video conferencing through Microsoft Teams; remember that this is an extension of the classroom and pupils should conduct themselves as they would in a classroom. This includes:

- Being on time for interactive session – you should aim to be there 5 minutes early.
- Trying to remain attentive during sessions and ensure that you are free from distractions. You may wish to use headphones to listen to the teacher in online sessions if it helps to avoid distractions.
- Not using personal social media in lesson time.
- All pupils should understand that these rules are designed to help keep them safe online and that if they are not followed, school sanctions will be applied and parents/guardians contacted.

Please indicate as a parent that you have read the above and shared with your son by placing a tick inside the box

Please sign below to give permission for your son to participate in interactive learning.

Name of your son ……..……..

Signed by Son ……..

Signed by Parent …….

Please return to cv19@hallschool.co.uk

2.7 Governing board

The governing board is responsible for:

- Monitoring the school's approach to providing remote learning to ensure education remains as high quality as possible
- Ensuring that staff are certain that remote learning systems are appropriately secure, for both data protection and safeguarding reasons

3. Who to contact

If staff have any questions or concerns about remote learning, they should contact the following individuals:

Here are some suggested issues and the most likely points of contact, but adapt and add to this as needed:

- Issues in setting work – talk to the relevant Head of Department, Deputy Head Learning and Teaching, Deputy Head of the JS or Head of Learning Support
- Issues with behaviour – talk to the Form Tutor, Head of Year, SLT
- Issues with IT – IT department techsupport@hallschool.co.uk
- Issues with their own workload or wellbeing – talk to their line manager, SLT, HR
- Concerns about data protection – talk to the data protection officer (Varsha Patel)
- Concerns about safeguarding – talk to the DSL (Willem Steyn)

4. Data protection

4.1 Accessing personal data

- When accessing personal data for remote learning purposes, all staff members will:
- Use either Microsoft One Drive to access files or use a remote server connection
- Staff may use their own devices to access data, however these should be secured (see 4.3). Where staff have a school device these should be used.
- Should you need to borrow a school laptop or any other technology for a period of RL please make the IT department/Varsha Patel aware as soon as possible so this can be organised and collected if necessary.

4.2 Processing personal data

Staff members may need to collect and/or share personal data as part of the remote learning system. As long as this processing is necessary for the school's official functions, individuals won't need to give permission for this to happen.

However, staff are reminded to collect and/or share as little personal data as possible online.

4.3 Keeping devices secure

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 the 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 antivirus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

- Using 2 factor authentication

5. Safeguarding

The move to online teaching and learning offers a different opportunity to interact with our pupils and students. As with any change in the way we do things, it's vital to ensure that we adapt our established policies and procedures to our new way of working. Here are ten key points to remember when we are working remotely:

We need to look after ourselves and each other as much as possible. If you feel that you need help or that a colleague needs help, please let someone know as quickly as possible. This could be via your HOD, Willem Steyn or Chris Godwin who can signpost you to sources of help. We will not be able to help pupils through the challenges we are all facing unless we are in a good place ourselves.

1. **Our existing policies (Safeguarding, ICT Acceptable Use Agreement, Social Media to name a few) are still in operation.** We must therefore ensure that we familiarise ourselves with these policies before they become inaccessible to us if working remotely.
2. **We must not communicate with pupils and students in a way which puts us at the risk of an allegation being made against us.** The yardstick here is that if we are using private channels such as the Class Notes function in Teams, we should be utterly professional in the comments we make and there should be no room for ambiguity. If we wouldn't write a comment on a piece of paper, it must not go online. If we are concerned about a pupil's comment or work, it should be screenshot and shared with a Form Teacher/ HOD/ Willem Steyn (please put on CPOMS which can be accessed from your phone, if relevant).
3. **We must be cautious of entering into unduly lengthy dialogue online with an individual pupil or student.** If a pupil attempts to engage in extensive dialogue in Class Notes, take the comment into the shared area (but anonymise it if necessary).
4. **We need to keep in touch with the pupils and students for whom we have a pastoral responsibility.** Primarily, this will happen with a scheduled form group (via Teams) every morning. A spreadsheet must be included in these form groups. A spreadsheet recording when contact has been made, and issues arising with each pupil, needs to be completed. If there is an *urgent* need for a call to be made via a private phone, the number must be withheld by dialling 141 first and a record of the call made (e.g. an email to Head and Willem to give the purposes of the call and any actions taken as a result of it.) Subject teachers should track which students are engaging in lessons and which are not? Please contact form tutors and parents if needed if certain students have not been engaging with your lessons.
5. **We must take care that any material provided to students to watch is age-appropriate. -** we must assume that pupils will be unsupervised when learning at home.
6. **We should model good online behaviour in all ways.** This includes the language we use to interact with pupils and colleagues (which should always be respectful and not resort to "banter") and not responding to comments from pupils between 9pm and 8am.
7. **We have a duty to report our safeguarding concerns about pupils via the normal channels.** This is likely to be a very anxious time for many pupils and we will need to support them as best we can through their difficulties. Willem will be monitoring CPOMS as regularly as she does when in school, so please raise concerns as soon as possible. If you do not receive a quick response, please act in accordance with the Safeguarding Policy.

6. **Roles and responsibilities**

At The Hall, we recognise the importance of an online safety strategy that is inclusive of the whole school community.

6.1 **Head teacher's role**

The Head teacher, along with the DSL has ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data
    - ensuring that online safety issues are given a high profile within the school community
    - linking with the board of governors and parents and carers to promote online safety and forward the school's online safety strategy
    - ensuring online safety is embedded in staff induction and training programmes
    - deciding on sanctions against staff and pupils who are in breach of acceptable use policies and responding to serious incidents involving online safety.

6.2 **Governors' role**

Governing bodies have a statutory responsibility for pupil safety and should therefore be aware of online safety issues, providing support to the head teacher in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep pupils safe online and that these are reviewed regularly.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, governors should always use business email addresses when conducting school business.

6.3 **Online safety co-ordinator's role**

The Hall has a designated online safety co-ordinator (Chris North Head of ICT) who is responsible for co-ordinating online safety policies on behalf of the school .The online safety co-ordinator is responsible for the following:

- to develop, implement, monitor and review the school's online safety policy
- to ensure that staff and pupils are aware that any online safety incident should be reported to them
- to ensure online safety is embedded in the curriculum
- to provide the first point of contact and advice for school staff, governors, pupils and parents

- ·to liaise with the school's network manager, the head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- to assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- to raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- to ensure that all staff and pupils have read and signed the acceptable use policy (AUP)
- to report annually to the board of governors on the implementation of the school's online safety strategy the DSL
- ·to maintain a log of internet related incidents and co-ordinate any investigation into breaches
- to report all incidents and issues to the DSL and Camden's online safety officer.

7. How will infringements be handled? –

N.B. This is tested out annually using www.360safe.org.uk as an Audit

STUDENT	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email • Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: SLT / Head of Computing
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email after being warned • Continued unauthorised use of mobile phone (or other new technologies) after being warned • Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups • Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc • Trying to buy items over online • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not logging off or notifying a member of staff of it	**Refer to Class teacher/ Head of Department / Head of Year / Head of Computing** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent] and SLT

STUDENT	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off). • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online. • Transmission of commercial or advertising material.	**Refer to Class teacher / Head of Year / Head of Computing / Head teacher / removal of Internet and/or Learning Platform access rights for a period** Escalate to: contact with parents / removal of equipment / SLT **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned. • Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent. • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998. • Bringing the school name into disrepute.	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP via DSL where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.	**Referred to SLT / Head teacher** Escalate to: *Warning given*

• Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school computer hardware or software; • Any deliberate attempt to breach data protection or computer security rules; • Deliberately creating ,accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent; • Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988; • Bringing the school name into disrepute	**Referred to DSL/ Head teacher / Governors;** **Other safeguarding actions:** ▪ Remove the PC to a secure place to ensure that there is no further access to the PC or laptop. ▪ Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school. ▪ Identify the precise details of the material. *Escalate to:* Report to Police / CEOP where child abuse or illegal activity is suspected.

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online Safety / Acceptable Use Policy. All staff will be required to sign the school's Online Safety acceptable use agreement form;

- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate Online safety / acceptable use agreement form;

- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents;

- Staff are issued with the 'What to do if?' guide on Online Safety issues.

8. Cyberbullying

8.1 DEFINITION OF CYBER-BULLYING

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself:

- By cyber-bullying, we mean bullying by electronic media;
- Bullying by texts or messages or calls on mobile phones;
- The use of mobile phone cameras to cause distress, fear or humiliation;
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites;
- Using e-mail to message others;
- Hijacking/cloning e-mail accounts;
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, Snapchat, Whatsapp, Bebo, Youtube and Ratemyteacher.

8.2 LEGAL ISSUES

Cyber-bullying is generally criminal in character. The law applies to cyberspace.
It is unlawful to disseminate defamatory information in any media including internet sites.

Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.

The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

The Malicious Communications Act (1988) – makes it an offense to send a letter, electronic communication or article of any description] which conveys—

(i)a message which is indecent or grossly offensive;

(ii)a threat; or

(iii)information which is false and known or believed to be false by the sender; or

- any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature.

8.3 POLICY

- The Hall School educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through Life Skills and in Online Safety lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.
- We train our staff to respond effectively to reports of cyber-bullying or harassment and has systems in place to respond to it. The school endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and filtering systems and no pupil is allowed to work on the internet in the Computer Room, or any other location within the school which may from time to time be used for such work, without a member of staff present. communications and regularly reviews the security arrangements in place.
- Whilst education and guidance remain at the heart of what we do, the school reserves the right to take action against those who take part in cyber-bullying.
- All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.
- The school will supports victims and, when necessary, will work with the Police to detect those involved in criminal acts.
- The Hall School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in or out of school.
- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the DSL/Headteacher any example of cyber-bullying or harassment that they know about or suspect.

8.4 GUIDANCE FOR STAFF

- As part of Education Act 2011, devices can be seized.
- If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones:

- Ask the pupil to show you the mobile phone – Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names.
- Make a transcript of a spoken message, again record date, times and names.
- Tell the pupil to save the message/image.
- Go with the pupil and see the DSL/Headteacher, or in their absence, a member of the SLT. Record on CPOMS

Computers:

- Ask the pupil to get up on-screen the material in question.

- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Accompany the pupil, taking the offending material, to see the DSL/ Headteacher.
- Normal procedures to interview pupils and to take statements will then be followed particularly if a child protection issue is presented.

8.5 GUIDANCE FOR PUPILS

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, matron or the DSLs or Headteacher.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your Class Teacher, parents/guardian or the DSL/Headteacher (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying).
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.

8.6 GUIDANCE FOR PARENTS

- It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. The Hall School informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying.
- Parents can help by making sure their child understands the school's policy and, above all, how seriously The Hall School takes incidents of cyber-bullying.
- Parents should also explain to their sons the legal issues relating to cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the DSL/Headteacher as soon as possible. A meeting can then be arranged with the DSL/Headteacher, which may involve other relevant members of staff
- If the incident falls in the holidays The Hall School reserves the right to take action against bullying perpetrated outside the school which spills over into the school.

8.7 PARENTS' USE OF SOCIAL MEDIA WEBSITES

- Any concerns that you may have, must be made through the appropriate channels by speaking to the class teacher, the DSL/Head Teacher or the Chair of Governors, so they can be dealt with fairly, appropriately and effectively for all concerned.
- Nationally, there is an increase in social media websites and group email being used to fuel campaigns and complaints against schools, Head Teachers, school staff, and in some cases other parents/pupils.

- The school considers the use of social media websites in this way as not in the best interests of the children or the school community.
- If slanderous or defamatory comments are posted on Facebook or other social network sites, the school will expect that any parent/carer or pupil responsible removes all comments immediately.
-

9: Use of New Technologies Policy for Parents/Carers

9.1 Aims

- To ensure that all children are safe within school
- To ensure that parents/carers do not endanger children (either their own or other people's) through the use of technology

9.2 Statement

- We understand that in this technological age that parents/carers make full use of modern technologies. We know that the majority of parents use technology responsibly. However, as a school there are now clear expectations for safeguarding and child protection relating to safe use of technology including the internet.
- In order to ensure the safety of all children the schools and governors require all parents of The Hall School to follow the guidelines laid down by the school.

9.3 Mobile Phones, Photos and Videos

The school acknowledges that special occasions in a child's life are significant and parents/carers may wish to record these moments.

Therefore school events e.g. whole school assemblies, can be recorded through videos and photos but, in order to safeguard all children, any photos or videos taken during events cannot be put up on You tube or any social networking sites
Parents/carers and their families are not permitted to send photos or information to the press

10: Communication and Mobile phone use relating to Staff

Copies of emails sent to parents need to be retrievable and easily accessible. Where possible they should be sent through iSams. Staff should respond to an email within 24 hours, if only a holding response, before a fuller reply within an agreed stated timeline. Staff should decide which other relevant staff should be copied in on responses and issues arising, including boy's form/class teachers. Staff involved in potentially tricky issues should involve other relevant senior staff to guide and advise.

Staff must not use personal email addresses or mobile phones / devices to communicate with pupils.

There may be other situations (e.g. school trips, away fixtures, weekend events) using professional judgment in which it may be helpful for staff to provide their mobile phone numbers to parents to help with the smooth running of an activity. School mobiles are also available.

- Staff must not put themselves in a position where they could be accused of improper behaviour by engaging in private online communications with pupils.
- Staff must not add or accept current or past pupils as 'friends' on any social networking site (including Instagram and Snapchat).
- Staff may have mobile phones.
- Staff are not to use mobile phones in the classroom, during lessons. Phones are to be on 'silent' or switched off during class time. Phones should not be used whilst on playground duty or during the teaching of a lesson outside.
- We expect staff to act in a responsible professional manner with regards to the use of mobile phones in school, including to facilitate communication on school business
- Calls/ texts must be made/ received in private during non-contact time. Calls should not be made on a mobile phone in the any of the staff rooms.
- Phones must be kept out of sight (e.g. drawer, handbag, pocket) when staff are with children.
- Staff should think about the images taken on a mobile phone and where they are kept. Images or film must be loaded within 24 hours on return to school to a school server and removed from the mobile phone / camera. It is advisable that where possible, photos should be taken on a school device.
- It is important that a mobile phone is available when a visit, event or sporting fixture is taking place away from school. A school mobile is available if required.
- Mobile phones, device and Satellite Navigation devices must not be used whilst driving minibuses.

The policy on the use of mobile phones and cameras also applies to the EYFS setting.

11: The Sharing of Youth Produced Sexual Imagery (sexting)

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photo and videos. Such imagery involving anyone under the age of 18 is illegal.

12: The Sharing of Youth Produced Sexual Imagery (sexting)

The practice of children sharing images and videos via text message, email, social media or mobile messaging apps has become commonplace. However, this online technology has also given children the opportunity to produce and distribute sexual imagery in the form of photo and videos. Such imagery involving anyone under the age of 18 is illegal.

12.1. Definition of Sexting

Sexting refers to both images and videos where:

- A person under the age of 18 shares imagery created by another person under the age of 18 with a peer under the age of 18; and
- A person under the age of 18 shares imagery created by another person under the age of 18 with a peer under the age of 18 or an adult; and
- A person under the age of 18 is in possession of sexual imagery created by another person under the age of 18.

12.2 Guidance for staff and procedures

- All incidents of this nature should be treated as a safeguarding concern.
- Cases where sexual imagery of people under 18 has been shared by adults and where sexual imagery of a person of any age has been shared by an adult to a child is child sexual abuse and should be responded to accordingly.
- If a member of staff becomes aware of an incident involving sexting they should follow the safeguarding procedures and refer to the DSL as soon as possible. The member of staff should confiscate the device involved and set it to flight mode or, if this is not possible, turn it off.
- **Staff must not view, copy or print the imagery.**
- The DSL will hold an initial review meeting with appropriate school staff and subsequent interviews with the children involved (if appropriate). Parents must be informed at an early stage and involved in the process unless there is reason to believe that involving parents would put the child at risk of harm.
- Immediate referral at the initial review stage should be made to Children's Services Local Referral, Intervention and Assessment Services Team, or the police as appropriate.
- Immediate referral at the initial review stage should be made to Children's Services Local Referral, Intervention and Assessment Service Team/police if:
    - the incident involves an adult;
    - there is good reason to believe that a young person has been coerced, blackmailed or groomed or there are concerns about their capacity to consent (for example, owing to special educational needs);
    - what is known about the imagery suggests the content depicts sexual acts which are unusual for the child's development stage or is violent;
    - the imagery involves sexual acts;
    - the imagery involves anyone aged 12 or under; and
    - there is reason to believe the child is at immediate risk of harm owing to the sharing of the imagery (for example the child is presenting as suicidal or self-harming).
- If none of the above applies then the DSL will use their professional judgement to assess the risk to students involved and may decide, with input from the Headteacher, to respond to the incident without escalation to Children's Services Local Referral, Intervention and Assessment Service Team, or the police.
- In applying judgement, the DSL will consider if:
    - there is a significant age difference between the sender / receiver;
    - there is any coercion or encouragement beyond the sender / receiver;
    - the imagery was shared and received with the knowledge of the child in the imagery;
    - the child is more vulnerable than usual (i.e. at risk);
    - there is a significant impact on the child involved;
    - the image is of a severe of extreme nature;
    - the child involved understands consent;

    - the situation is isolated or if the image been more widely distributed;
    - there are other circumstances relating to either the sender of recipient that may add cause for concern (i.e. difficult home circumstances);
    - the children have been involved in incidents relating to youth produced imagery before.
- If any of these circumstances are present the situation will be escalated according to the school safeguarding procedures, involving reporting to the police or children's social care. Otherwise, the situation will be managed within the School.
- The DSL will record all incidents of sexting, including both the actions taken, actions not taken reasons for doing so and the resolution in line with safeguarding recording procedures on CPOMS.