Longman's Hill Community Primary School

Online Safety Policy – October 2025

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2025 (KCSIE), 'Teaching Online Safety in Schools' 2023, statutory RSHE guidance 2025 and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

This policy applies to all members of the Longman's Hill School community (including teaching and support staff, supply teachers, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role. It should be read in conjunction with the school's behaviour, child-protection, sex and relationships and social media policies.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The school will deal with such incidents within the procedures set out in the online policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

Today's children's daily use of the Internet and digital technologies represents a seamless extension of their physical world as well as their emotional lives and their development. As online content, social networks and instant messaging converge with mobile technology to produce lives which are always 'on', any line which may have existed between being online and offline is disintegrating.

For the majority of children and young people, internet technologies are not a 'new thing' as they are for many adults. They are simply another part of the world they have grown up with. Despite this, all who provide services and support to children and young people must recognise that for many children technology is now an important, if not the main way, in which they send and receive information, access entertainment and, perhaps most importantly, communicate with people.

The online safety policy encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

Our school believe that in order to maximize the opportunities within this technological environment, whilst minimizing the potential risks, we must encourage children and young people to develop as responsible online citizens. Children must be taught to recognise their responsibility to keep themselves safe online as well as accepting the responsibility they have to present themselves as positive role models. It is only through the development of a sense of online responsibility that we can ensure the safety and wellbeing of today's children and young people.

TEACHING AND LEARNING

Why is Internet use important?
The rapid developments in electronic communications are having many effects on society.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for children who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- the possibility of educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils, provided by a local authority firewall.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

What are the potential risks of internet and social media use?

Online-safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct or Commerce (see KCSIE 2025). 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 41% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months. See the full reports here Ofcom Report on children's media use.

KCSIE 2025 highlights additional risks e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families, including sexual and criminal exploitation, serious youth violence, upskirting and sticky design.

Following covid, more time has been spent online increasing the risk for grooming and exploitation (CSE, CCE and radicalisation) and potentially reducing opportunities to disclose such abuse.

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

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm
- Commerce: behaviour online linked to gambling

Some of the risks users may face include:

- Access to illegal, harmful or inappropriate images or other content (including radicalisation /extremism material and pornography)
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images with and without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/Internet games/ websites
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- Generating large bills through overuse of their mobiles, gaming etc

Roles, Responsibilities and Training

This school is a community, and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Depending on their role, all members of the school community should **read the relevant section in Appendix 1 of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions in the annex.

Online safety is everyone's responsibility within school. However, governors have a statutory duty to ensure that online safety procedures remain upto date, are adhered to and monitored. The headteacher is the designated safeguarding lead.

Staff receive face to face safeguarding training once every year. They also receive a monthly online safeguarding newsletter and access to additional training from Knowsley Learning partnership.

Pupils are taught specifically about how to keep themselves safe when on the internet through a well-planned curriculum that is age appropriate based on the needs of the pupils.

Education & Curriculum

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of the PSHE and assembly programme and is regularly revisited in Computing and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in school and outside of school. It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

- A range of safeguarding issues are considered as part of the online safety education: keeping their personal information private, healthy relationships on and off line, grooming, sending inappropriate images and the consequences of this, gaming, gambling, radicalisation and how to recognise the signs and keep themselves safe
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

See appendix 1- Roles and responsibilities

MANAGING INFORMATION SERVICES TO MINIMISE RISK

This section of the policy contains information about how we will manage users and sets out what we consider to be acceptable uses for a range of technologies.

'Data protection: a toolkit for schools' (August 2018) states:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.**"

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of 'Egress' to encrypt all non-internal emails is compulsory for sharing pupil data and safeguarding information. If this is not possible, the 'encrypt' tool in Office Outlook360 must be used.

Maintaining ICT system security.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage facilities by pupils within school is prohibited to protect against virus transfer.
- Files held on the school's network will be regularly checked.
- The ICT Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- See Appendix 2 showing which technologies are permitted for use by staff and pupils at Longman's Hill School

Managing Filtering of Inappropriate Content

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided through North Yorkshire County council. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering and monitoring system called Smoothwall.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

- The school will work in partnership with parents and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The Local Authority provide a firewall which effectively filters unsuitable websites.
- Our school additionally pays for Smoothwall monitoring, which give live-time alerts when pupils attempt to access unsuitable websites or materials. The DSL will always follow this up with a conversation with the pupils and follow safeguarding protocols where necessary.
- In the unlikely event that staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader. Children will be taught to turn off the screen only if they come across unsuitable sites.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the IWF Internet Watch Foundation) or CEOP (Child Exploitation and Online Protection).

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phones will not be used by staff during lessons. The sending of abusive or inappropriate text messages is forbidden.
- Instant messaging will not be permitted.
- Pupils are not permitted to wear internet- capable watches.

How should personal data be protected?

The headteacher and governors will ensure frameworks are in place for the protection of data and of safeguarding information sharing.
They will ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Appropriate use of websites

- All staff and pupils will be expected to sign and adhere to an 'Acceptable Use Policy' – see appendices 3 and 4
- Staff will be aware of which activity is illegal and therefore obviously banned and possibly lead to criminal prosecution. They will also be aware of other activities which may generally be legal but which would be inappropriate in a school context. See Appendix 5- Unsuitable / inappropriate Activities on the internet.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use; processes are in place for dealing with any unsuitable material that is found in Internet searches – children will turn off screen and inform adult. Staff will notify safeguarding lead immediately who will contact Schools ICT for further support in filtering / blocking the content or site.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with pupils who may misinterpret information
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research
- All users must observe copyright of materials published on the Internet
- Teachers will carry out a risk assessment regarding which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed.
- All internet use at school is monitored and logged; staff and pupils are made aware of this. The school only allows the ICT technician and headteacher to access these logs.

Appropriate use of mobile phones and wearable technologies

- In the event that staff use personal mobile devices to contact parents / carers, in connection with school business or activities, they must ensure their mobile number is blocked/ hidden. Under no circumstances should a pupil or parents/carers be given a member of staff's personal mobile number
- Staff should not use personal mobile phones in school during working hours when in contact with children. However, staff can access phones at break / lunch, including to access school communications using Microsoft Teams. Phones must be left on silent.
- Child/staff data should never be downloaded onto a private phone.
- Staff can use the school wifi to access the internet on their personal device in breaks / lunch. However, any personal use and access to websites must be in line with the conditions listed in the Acceptable Use Policy.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- Pupils are not permitted to have mobile phones in school except where agreed. In such cases, pupils must hand the phone to the school office at the start of the day where it will remain until the end of the school day.

- **Parents** must not take any photos in classrooms during events such as 'maths mornings' or 'stay and create'. When at school events, parents may take photos of their own child for personal use only and must ensure no images of other children are used on social media sites. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Appropriate use of E-mail

- Pupils **do not** have access to their own school-based email account.
- Any emails sent by children will be directly linked to curriculum learning and will use the school e mail address. Teachers will be responsible for checking the content of any e mails, prior to sending.
- Children will not divulge ANY personal information in e mails which may result in them being identified. First names only will be used.
- The forwarding of chain messages is not permitted.
- Digital communications by staff with parents / carers (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems. Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- The school's e-mail service should be accessed via the provided web-based interface by default
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courteous and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system
- If data or safeguarding information needs to be shared, where possible Egress will be used.

Appropriate use of Social Media

We try to manage our online reputation because negative coverage almost always causes some level of disruption. We manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner, even though there are no official/active school social media accounts.

Staff, Pupils' and Parents' Social Media Presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

- Parents / carers and pupils will be informed that they do not use social media to criticise or make inappropriate comments about the school, an individual member of staff or another pupil as making defamatory comments online has exactly the same legal consequences as if they are made directly to

someone else. Similarly threats of violence can lead to criminal proceedings under the Malicious Communications Act. If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed.

- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the new Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

- The school will block access to social networking sites. However, pupils will be taught about online safety when using social networking sites
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended or e-mail 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 background detail in a photograph which could identify the student or his/her location eg. House number, street name or school.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for children to use on a personal basis.
- Staff should not access social networking sites on school equipment in school or at home that have not been pre-approved by the school
- Staff users should not refer to any member of staff, pupils, parents/carers, the school or any other member of the school community on any social networking site or blog in a derogatory way

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy

- Pupils/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other pupils or members of the school community

Appropriate use of Removable Data Storage Devices

- Any memory / removable data devices/ USB pens used by staff must be encrypted
- Any information that is on removable data storage device for school use should not be transferred onto any personal devices, in particular any information that is covered by the data protection act and could lead to an individual being identified
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using school provided anti-virus software before run, opened or copied/moved on to local/network hard disks
- Pupils should not bring their own removable data storage devices into school for use on school equipment.
- Staff are encouraged to use 'the cloud' to save and access information which gives them a direct link to data/ documents stored on the school's virtual server.

Appropriate use of School ICT Equipment
Devices used at home should be used just like if they were in full view of a teacher or colleague.

- Privately owned ICT equipment should never be connected to the school's network and no personally owned applications or software packages should be installed on to school ICT equipment
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted
- If staff are working on confidential documents, all should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access
- If the school provides ICT equipment for pupils to use at home this needs to be part of the pupil and parent/carer AUP to ensure it is only used for school work and only suitable resources are accessed on the device. The device will be set up to minimise the pupil being able to access any inappropriate information. Parent/ carers will also be asked to set up parental controls on their own broadband provider to try to prevent pupils accessing inappropriate materials and guidance will be provided on how to do this.

There will be a specific focus on SEND pupils who are often provided with technology to support their learning. This is not applicable at Longman's Hill at the moment.

Managing Content on the School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Jan Elcock and Linda Richardson. The site is managed by / hosted by Colourscope. Class teachers also have access and can update their class and subject pages.

- Schools have the same duty as any person or organisation to respect and uphold copyright law
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).
- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.
- The Website complies with the Local Authority guidelines for website content.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Appropriate use of digital images, videos and work, including those of pupils.

The school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information, for example through an active school website which are used to inform, publicise school events and celebrate and share the achievement of students.

- Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be used. This list is held in the school office.
- Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file
- Visitors / contractors will be asked not to use their mobile phone whilst on site with any pupils presence due to all mobile phones containing a camera

MANAGING REPORTS OF MISUSE

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

School procedures for dealing with online-safety are detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies

- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also follow the Whistleblowing Policy.

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below)

Incident Reporting
Any online safety incidents must immediately be reported to the designated safeguarding lead (headteacher) who will investigate further and notify Schools ICT.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse.

Appendix 6 and 7 outline the responses that will be made to any apparent or actual incidents of misuse from pupils and staff. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials, the headteacher will liaise with the Police and seek advice. Actions will be followed in accordance with advice, in particular with regards to the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

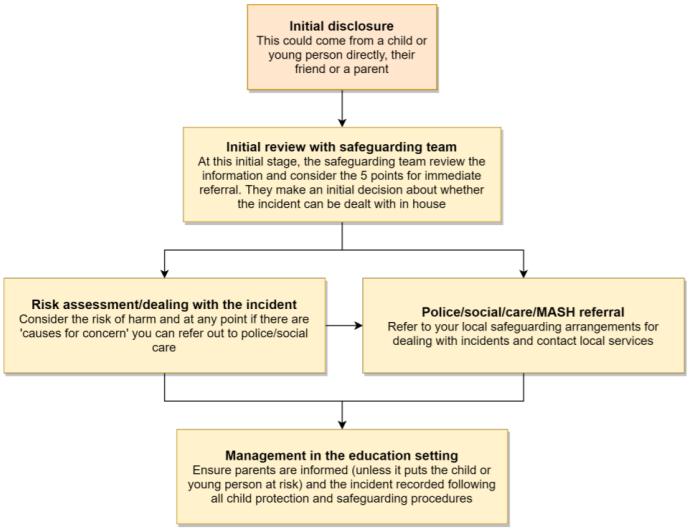
The information in the sections below outlines how specific issues and concerns can be dealt with.

Sexting – sharing nudes and semi-nudes

1) All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.
2) There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an

incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

3) The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



4)

5) ***Consider the 5 points for immediate referral at initial review:**

6) 1. The incident involves an adult

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

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

9) 4. The images involves sexual acts and any pupil in the images or videos is under 13

10) 5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

11)

12) It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

13) The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

Sexual Violence and Harassment

DfE guidance on sexual violence and harassment has now been incorporated into Keeping Children Safe in Education and is no longer a document in its own right. It would be useful for all staff to be aware of this updated guidance: Part 5 covers the immediate response to a report, providing reassurance and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here (and probably is)'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices/ systems/networks/platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property. Children are allowed to bring mobile phones to school but they must be handed in to the school office at the start of the day. Smart watches (with internet connectivity and cameras) are not allowed to be worn by pupils.

Social Media Incidents

See the social media section in this document for rules and expectations of behaviour for children and adults in the Longman's Hill School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Searching and Confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

When considering an online safety incident involving a pupil(s) a school does need to take into account the nature of the incident, the age of the child and if there is a need to involve any partner agencies.

- Sanctions available include:
  - interview/counselling by senior member of staff/class teacher/teaching assistants;
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

Professionals in all agencies have a responsibility to refer a child to Children's Social Care (part of the Children and Families Service)/Disabled Children's Service when it is believed or suspected that a child:

- Has suffered significant harm and /or;
- Is likely to suffer significant harm and/or;
- Has developmental and welfare needs which are likely only to be met through provision of family support services (with agreement of the child's parent).

- **Contact details:** By Phone: 01609 780780 Email:social.care@northyorks.gov.uk

POLICY DECISIONS

How will Internet access be authorised?

- All staff and pupils will initially be granted Internet access.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. Filtering and monitoring is provided by North Yorkshire Schools ICT Smoothwall.
- However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

COMMUNICATION OF THIS POLICY

How will the policy be introduced to pupils?

- Internet safety guidelines will be prominently linked from the school website (Children's Learning Zone) Internet sites.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use will accompany Internet access.

How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Leadership Team.
- Staff training in safe and responsible Internet use, and on the school e-Safety Policy will be provided as required (including in annual September training)
- This policy forms part of the induction process for all new staff (including temporary, long-term supply and non-classroom based staff including those starting mid-year).
- It will be clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school

How will the policy be discussed with parents?

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This may include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home.

The e–Safety Policy and its implementation will be reviewed annually.
Our School Policy has been approved by Governors.
The School has appointed a member of the Governing Body to take lead responsibility for e-Safety

The School e-Safety Coordinator/ DSL is Mrs Jan Elcock
The DDSL is Mrs Liz Rhodes
The link governor for safeguarding is Mrs Lyndsay Muschamp
The School e-Safety Governor is Mrs Sue Porter
Policy approved by Head Teacher: …… Date: ……
Policy approved by Governing Body: …….. Date: ……

Appendix 1
Roles and Responsibilities

Of Governors:

- Approve this policy and strategy and subsequently review its effectiveness.
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Ensure appropriate filters and appropriate monitoring systems are in place being "careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding".
- Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 and 5 of KCSIE; SLT and all working directly with children have read Annex B
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

Of the Headteacher:
Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school's arrangements
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including remote systems are implemented according to child-safety first principles
- Liaise with technical colleagues on a regular basis to have an understanding and awareness of filtering and monitoring provisions and manage them effectively
- Carry out online searches with consistent guidelines as part of due diligence for the recruitment shortlist process

- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure the school website meets statutory requirements
- Supporting the Governors comply with the online safety aspects of the Keeping Children Safe in Education documentation
- The safety (including online safety) of all members of the school community.
- Effective and regular training about online safety is provided for the whole school community and a log is kept of the staff who complete the training
- Effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues
- There are effective procedures in place the event of an online safety allegation which are known and understood by all members of staff
- Establishing and reviewing the school online safety policy and documents and making them available on the school website

Of the Designated Safeguarding Lead

- The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection including online safety.
- Work with technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards, whenever school devices are loaned for home-learning.
- Ensure an effective whole school approach to online safety that empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.
- Ensure ALL staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated
- Liaise with the Chair of Governors to ensure that ALL governors and trustees undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Work with the DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents.

- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. send secure message to teacher via Google Classroom
- Oversee 'appropriate filtering and monitoring' with governors. Liaise with technical teams and ensure they are implementing not taking the strategic decisions on what is allowed and blocked and why. Also, as per KCSIE be careful that 'over blocking' does not lead to unreasonable restrictions.
- Facilitate training and advice for all staff, including supply teachers:

Of all staff:

In addition to the elements covered in the Staff Acceptable Use Policy (AUP), all staff are responsible for ensuring that:

- Read and follow this policy in conjunction with the school's main safeguarding policy and the relevant parts of Keeping Children Safe in Education
- Understand that online safety is a core part of safeguarding and part of everyone's job – never think that someone else will pick it up. Safeguarding is often referred to as a jigsaw puzzle – you may have the missing piece, so do not keep anything to yourself. Record online-safety incidents in the same way as any safeguarding incident; report in accordance with school procedures
- Know who the Designated Safeguarding Lead (DSL) and Deputy DSL are (Jan Elcock and Liz Rhodes); notify them not just of concerns but also of trends and general issues you may identify. Also speak to them if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Sign and follow the staff acceptable use policy and code of conduct.
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHCE curriculum, both outside the classroom and within the curriculum, supporting subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites
- Follow best-practice pedagogy for online-safety education, avoiding scaring, victim-blaming language and other unhelpful prevention methods.
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and classroom resources before using for accuracy and appropriateness.
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Take a zero-tolerance approach to all forms of child-on-child abuse, not dismissing it as banter - this includes bullying, sexual violence and harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues

- Model safe, responsible and professional behaviours in your own use of technology. This includes outside school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- They do not 'be-friend' any pupil or pupil family member on social media in a social context whilst the pupil is at the school
- All staff should be aware that emails can be part of Freedom of Information requests so all correspondence needs to be professional, courtesy and respectful
- If confidential information / information under the data protection act is being sent by email it must be sent through the secure email system which if provided by Schools ICT would be the Egress system which the schools administration and headteacher have access to but more licenses can be purchased.

Of the Technical Service Provider (SchoolICTS) :

- Ensure the school's ICT infrastructure is secure and meets requirements for filtering and monitoring
- Ensure the school's website is kept secure from 'hacking' and there is an action plan in place if it is hacked
- Ensure the school's password policy is adhered to
- Ensure the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Keep up to date with online safety technical information
- Ensure the use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the named SLT for action.
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.

Of All Pupils

- Be responsible for using the school ICT systems in accordance with the Pupil Acceptable Usage Policy, which they will be required to sign before being given access to school systems. Parents/carers will be required to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy also covers their actions out of school, including on social media.
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Of all parents/carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. Schools will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Usage Policy and will alongside this sign the Parents Acceptable Usage Policy
- Ensuring that they do not use social media to criticise or make inappropriate comments about the school or an individual member of staff as making defamatory comments online has exactly the same legal consequences as if they are made directly to someone else. Similarly threats of violence can lead to

criminal proceedings under the Malicious Communications Act. If as a parent/ carer they have any concerns about anything which happens in schools then please contact the school directly.

- Talk to the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning, whether for homework or during any school closures or isolation and flag any concerns
- Support the child during any home learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

Parents and Carers should also be aware of the health effects of children and young people having too much 'screen time'. This can limit the amount of time children are being physically active, reduce the amount of time they are sleeping and could be impacting on their eyesight. A number of systems and apps are available that can limit the screen time for children and young people alongside parents and carers talking to their children about the issues.

There are links from our school website (www.longmanshill.co.uk) to websites which can support and advise parents regarding online safety under the 'Statutory Information/ safeguarding' tab.

Appendix 2
Permitted technologies – staff and pupils

Communication Technologies	Permitted	Permitted at certain times	Permitted for named staff	Not Permitted	Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones may be brought to school	✓						✓	
Mobile phones used in lessons				✓				✓
Use of mobile phones in social time	✓							✓
Staff contacting a pupil on a mobile phone				✓				
Taking photographs/film on personal mobile devices / digital camera				✓				✓
Taking photographs/film on school mobile devices / digital camera for school purposes only	✓						✓	
Parent / carer taking photos of a school event on their own device and uploading online with public access				✓				✓
Use of personal tablets/ laptops ipads etc in school				✓				✓
Use of school owned tablets/ laptops/ ipads in school but not for personal use	✓				✓			
Use of school owned tablets/ laptops/ ipads out of school but not for personal use	✓ with AUP						✓ Eg trips	
Only using school provided encrypted storage devices	✓				✓			
Use of school email for personal emails				✓				
Social use of chat rooms/facilities				✓				✓
Use of social network sites in school				✓				✓
Use of educational blogs	✓						✓	

Appendix 3 Acceptable Internet Use Policy – Pupils

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents or in the event of illegal activities contact with the police.

- I will only access the school network through my authorised username and password. I will not use the passwords of others.
- I will not use the school IT systems / devices for personal or recreational use, for accessing social media sites, on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any school computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/ipod) in school at times that are permitted. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends'.
- I will not take, or distribute, images of anyone else without their permission.
- I will not take, or distribute, images of myself or anyone else semi-naked or naked.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Pupil Signed ……..
Date …….
Parent / Carer Signed ……..
Date……

Appendix 4

Acceptable Internet Use Policy – Staff and other adults in school and Governors

Responsible Use Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the school ICT systems (e.g. laptops, email, Learning Platform etc.) out of the school.
- I will only use school ICT equipment / mobile phones for school purposes I will not use any personal devices for any school business
- I understand that the school ICT systems are intended for educational use and that I will not use systems for personal or recreational use.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the appropriate person

I will be professional in my communications and actions when using school ICT 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 am aware that emails can be part of Freedom of Information requests so all my correspondence will be professional, courtesy and respectful
- 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.
- I will not use chat and social networking sites in the school in accordance with the school's policies.

I will only communicate with student 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.
- I will not befriend any present pupil or their family members on social media
- I will not 'discuss' any school issues on social media
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, 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 policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 (unless I have permission) 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, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport and hold data about others that is protected by the Data Protection Act in an encrypted manner. I will not transfer any data to any personal devices.
- I understand that data protection policy requires that any staff or learner 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 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 ICT equipment in school, but also applies to my use of school ICT systems and equipment out of the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 ICT systems (both in and out of school) within these guidelines.

Staff/Volunteer/ Governor

Name ……..

Signed …….

Date …….

Appendix 5

Appropriate / inappropriate Internet Activity

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable AND illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography					✓
Promotion of any kind of discrimination				✓	
Any Hate Crime – motivated by hostility on the grounds of race, religion, sexual orientation, disability or transgender identity.					✓
Promotion of any kind of extremist activity					✓
Promotion of racial or religious hatred					✓
Accessing any extremist materials online (e.g Far Right Extremism)				✓	
Threatening behaviour, including promotion of physical violence or mental harm					✓
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	

e.g discussing school issues on social media					
Using school systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				✓	
Creating or propagating computer viruses or other harmful files				✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
On-line gaming (educational)		✓			
On-line gaming (non-educational)				✓	
On-line gambling				✓	
On-line shopping / commerce			✓		
File sharing			✓		
Use of social networking sites			✓		
Downloading video broadcasting e.g. Youtube for educational purposes	✓				
Uploading to video broadcast e.g. Youtube			✓		

Appendix 6
Incidents involving pupils and actions to be taken

Incident involving pupils – either in school or out of school – it could be a concern raised by a friend/ parent	**Teacher to use school behaviour policy to deal with**	**Refer to Senior member of staff**	**Record and monitor the pupils behaviour and refer to external agencies if required**	**Refer to technical support staff for action re security/filtering etc**
A concern raised by a pupil/ teacher / friend/ parent (carer). A pupil need positive support – Signs of grooming Signs of peer on peer abuse / grooming / power domination Signs of radicalisation Signs of CSE Signs of cyberbullying		✓	✓	
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓			✓
Unauthorised use of mobile phone/ digital camera/ other handheld device.	✓			
Unauthorised use of social networking/ instant messaging/ personal email and online gaming	✓	✓		✓
Unauthorised downloading or uploading of files		✓		✓
Allowing others to access school network by sharing username and passwords		✓		✓
Attempting to access or accessing the school network, using another student's account		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff		✓		✓
Corrupting or destroying the data of other users		✓		✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓		✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓		✓
Using proxy sites or other means to subvert the school's filtering system		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓		✓

Appendix 7

Incidents involving members of staff and actions to be taken

Incident involving staff / adults in school	Refer to the headteacher *see below	Refer to technical support staff for action re filtering / security	Potential Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓		✓
Excessive or inappropriate personal use of the internet/social networking sites/ instant messaging/ personal email	✓	✓	✓
Unauthorised downloading or uploading of files	✓	✓	✓
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	✓	✓	✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓		✓
Deliberate actions to breach data protection or network security rules	✓	✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓
Using personal email/ social networking/ instant messaging/ text messaging to carrying out digital communications with students/ pupils	✓	✓	✓
Actions which could compromise the staff member's professional standing	✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓		✓

*In event of breaches of policy by the Headteacher, refer to the Chair of Governors.