Online Safety Guidance for Schools and Settings in North Yorkshire Updated September 2019

This guidance document is to enable schools and settings to develop and agree an effective approach to online safety for the whole school community.

Aims of the guidance document
This document has been developed in partnership between Education and Skills (NYCC), Inclusion Education (NYCC), the North Yorkshire Safeguarding Children Partnership (NYSCP), North Yorkshire Police and Schools ICT. The document sets out the statutory requirements for schools and settings alongside the roles and responsibilities for different members of the school community, the range of issues that need to be considered and signposting to further resources. The overall aim is that all schools and settings have implemented an effective online safety policy that meets the requirements for their school community.

Consultation
It is good practice to consult with the whole school community when developing or reviewing the school's online safety policy and provision. The following are prompts to support this process:

- How are pupils, parents/carers, governors, staff, partners and stakeholders going to be consulted and involved in the development / review of the policy and provision?
- Are all staff aware of the policy and provision? Has it been discussed at a whole staff meeting?
- How will the policy and provision be disseminated to the whole school community including external providers to ensure their contribution adds value to the online safety curriculum?

Training
The Education and Skills team provides high quality staff training to support schools in providing effective online safety policy and provision. The trainer is highly experienced and is a CEOP trained ambassador. A whole days training to support schools deliver effective online safety runs every academic year. Bespoke training can also be delivered to a school / cluster of schools as a twilight training session or on a school training day. Information on the training available can be accessed at www.nyeducationservices.co.uk

For further information and support please contact: Clare Barrowman, Health and Well-Being Adviser, on 01609 536808 or via email at clare.barrowman@northyorks.gov.uk

Teaching online safety in school, non –statutory guidance supporting schools to teach their pupils how to stay safe online within new and existing school subjects states;

- Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities but also challenges and risks
- Schools should be equipping pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world

Keeping Children Safe in Education, 2019 clearly states that:
The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

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

- **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Please see page 18 onwards for further information on a range of risk factors within these three categories and signposting to supporting guidance.

Online Safety Policy
It is essential that schools and settings have an online safety policy and it is read and used in conjunction with other school policies; specifically the anti-bullying, information (data protection) policy, behaviour, child protection / safeguarding, relationships and sex education and a clear

policy on the use of personal mobile technology in the school. Many pupils have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school should carefully consider how this is managed on their premises.

The policy needs to set out who it applies to:

- All members of the school and setting community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school. As well as use of personal technology whilst on the school premises or engaged in school activities. Many schools are providing information to external visitors when they sign in at school about the expected behaviours in relation to personal technology.
- 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 should 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.

An accessible online safety policy template

This is a guidance document not an online safety policy template. A policy template to support a school develop a policy can be accessed from the School Online Safety Policy Template. School's needs to ensure that they take into account all the key aspects identified in this guidance document and that a school personalises the policy to meet the needs, ethos and circumstances of their school.

Roles & Responsibilities of members of the school community;

The Governing body:

Governors are responsible for the approval of the online safety policy, ensuring it is disseminated to the wider school community and for reviewing the effectiveness of the policy. It is recommended that there is a named member of the Governing Body who takes on the role of online safety governor who has accessed training about online safety. To support governing bodies the following document may be a useful tool. Online safety in schools and colleges: Questions from the Governing Board - Questions that school governors should ask to help ensure their school leaders are keeping children safe online.

The role of the governing body does include ensuring that the statutory requirements of Keeping Children Safe in Education (Sep 2019) are complied with. In relation to online safety this includes:

- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description and they are able to access training so they:
  - have undertaken Prevent awareness training.
  - are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college;
  - can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and

radicalisation and are confident they have the capability to support SEND children to stay safe online

- A staff behaviour policy (sometimes called the code of conduct) should, amongst other things, include: acceptable use of technologies, staff/pupil relationships and communications including the use of social media
- Ensure that as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
- Ensuring that pupils are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through Relationships Education and Relationships and Sex Education (formerly known as Sex and Relationship Education), tutorials (in colleges) and/or where delivered, through Personal, Social, Health and Economic (PSHE) education. The Government has made regulations which will make the subjects of Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils in state-funded schools) mandatory from September 2020.
- Have in place policies and procedures on sexual harassment and peer on peer abuse that can occur online and offline.
- As schools increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. A school needs to ensure the appropriateness of any filters, monitoring and security systems which will be informed in part by the risk assessment required by the Prevent Duty but being careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding'.

- Regular monitoring of online safety incident logs and responding appropriately to the identified needs
- Ensure the company who is hosting the schools website has enough security in place so it cannot be inappropriately accessed and to have an action plan if it is 'hacked' e.g who regular checks the website including during school holidays, who is the key contact if the website is hacked
- The UKCCIS Education Group has developed a range of guidance for school governors to help governing boards support their school leaders to keep children safe online which can be accessed at https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Further support on appropriate filtering and monitoring

The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like both for schools/ settings and for providers of internet services in schools. These documents will provide a useful checklist when a school reviews the appropriateness of their present systems. All documents can be accessed from UK Safer Internet Centre Guidance on e-security is available from the National Education Network-NEN.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors should consider a whole school or setting approach to online safety. This will include a clear policy on the use of mobile technology in the school or setting. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school should carefully consider how this is managed on their premises.

A resource that could support a school review their online safety policy and practice is the 360 degree safe self-review tool, it is free to use and provides:

- Information that can influence the production or review of e-safety policies and develop good practice
- A process for identifying strengths and weaknesses
- Opportunities for commitment and involvement from the whole school
- A continuum for schools to discuss how they might move from a basic level provision for online safety to practice that is aspirational and innovative.

A resource to support Early Years setting review their policy and practice is also available

The Governors and Headteacher need to ensure that the online safety policy is crossed referenced with the information policy (data protection) with particular reference to no member of staff or governing body taking data outside of the school system and complying with GDPR. The policy needs to consider how information is shared/accessed with staff and the governing body for example all staff / governors being issued with a school email address, accessing information through a shared 'storage cloud', or on a secure part of the school website or being provided with an encrypted memory stick. These systems need to be agreed and adhered to by all staff / governors. It is recommended that all staff / governors sign an acceptable use policy (see appendix 6 for model AUP). Further information for governors about information governance can be accessed at http://cyps.northyorks.gov.uk/information-governance-schools

Roles & Responsibilities of the Headteacher:

- Supporting the Governors comply with the online safety aspects of the Keeping Children Safe in Education
- Supporting the Governors comply with the online safety aspects of the statutory regulations which will make the subjects of Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils) mandatory from September 2020.
- The 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
- Governors are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety education or safeguarding.
- Effective communication with parents/ carers about safe practices when using online technology's and support them in talking to their children about these issues
- Effective filtering, monitoring and security systems are set up
- There are effective procedures in place in 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
- The school's Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection issues that could arise through the use of ICT.

Roles & Responsibilities of a named member of the Senior Leadership Team:

- Liaising with staff, ICT Technical staff, online safety governor, SLT and partner agencies on all issues related to online safety

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Providing training and advice for staff and keeping a log of staff who complete training about online issues
- Keep a log of staff, pupils and families who have signed the Acceptable Use Policy (AUP) for the safe use of technology
- Receive and respond to reports of online safety incidents and creates a log of incidents and outcomes to inform future online safety developments
- Co-ordinating and reviewing online safety education programme in school (or working in partnership with the Personal, Social , Health, Education (PSHE) and/ or Computing lead) and ensuring the statutory requirements of the Relationships, Relationships and Sex Education and Health Education curriculum are being implemented by September 2020 which include online safety learning outcomes.

Roles & Responsibilities of the ICT technician:

- The school's ICT infrastructure is secure and meets requirements for filtering and monitoring
- The schools website is kept secure from 'hacking' and there is an action plan in place if it is hacked
- The school's password policy is adhered to
- 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
- Keeps up to date with online safety technical information
- 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.

Roles & Responsibilities of all staff:

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

- They have an up to date awareness of online safety matters and of the schools current online safety policy and practices
- They attend the training provided by the school about online safety and all new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy, Acceptable Usage and Child Protection Policies.
- They have read, understood and signed the school Staff Acceptable Usage Policy (AUP)
- 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
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Ensure that pupils understand and follow the school's online safety and acceptable usage policies
- Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended school activities
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- 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

The updated Guidance for Safer Working Practice for Adults who work with Children and Young People in Education, Section 12 focuses on 'Communication with children (including the use of technology)' For staff the guidance now reads:

- not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work
- not give out their personal details
- use only the equipment and internet services provided by the school or setting, unless school policies state otherwise
- only use internet-enabled personal devices in line with school acceptable use policies
- follow their school / setting's acceptable use policy and online safety guidance

Safer Internet have produced various supporting guidance and documents for staff who work in schools to enable them to help young people to stay safe online but also to ensure they protect their own online reputation, particularly when using social networking sites.
http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

Roles & Responsibilities of all pupils;

- Pupils are 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.
- Pupils have an entitlement to online safety education that will support them in staying safe when online using a range of technology and signposting to further advice and information. (This will be statutory for all pupils from September 2020).
- 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, if related to their membership of the school or using equipment provided by the school.

Roles & Responsibilities 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/ Carers Acceptable Usage Policy
- Access the school website and correspond with the school in accordance with 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.

Parents and Carers should also be aware of the possible 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.
These following websites provide supporting information for parents / carers to enable them to protect their children through setting up parental controls and being able to talk to their children about how to stay safe online. This information should be available on the school website for parents/ carers to access and they should be informed that the information and support is available for them.

NSPCC online safety	Provides helpful advice and tools that a parent/carer can use to help keep their child safe whenever and wherever they go online. • Has material and information for use with young children as well as older children • Key advice for parents / carers • Information on a range of social media sites and games
Net Aware	NSPCC in partnership with O2, provides useful information for parents about the most popular and current sites, apps and games used by children. The free tool is updated regularly. In addition, each site/app/game has free advice from O2 on how the privacy settings work for that particular platform.
Thinkuknow	Provides helpful advice and tools that a parent/carer can use to help keep their child safe online. They have downloadable guides for parents/ carers on various social media sites like: Instagram, Whatsapp, youtube etc They also have some useful films for parents to watch about the risks online and four specific films about sexting / 'self nudies' and how to talk to their children about this issue and what to do if this happens.
Childnet The whole website can be read in a variety of languages.	A range of information to support parents/ carers keep their children on safe including: • Parents: Supporting Young People Online (Leaflets in a variety of languages) • Key advice for parents / carers • Conversation starters to enable parents /carers to talk to their children • How to set parental controls on a range of devices • Gaming
Safer internet	Very specific advice, films and signposting to ensure parents/ carers have the information about how to set up parental controls on a range of devices and their home internet
Internet matters	Provides a wealth of information for parents/ carers on internet safety starting for parents and carers of 0-5 years olds working upwards. Information, films and advice about parental settings and information about a range of games and apps that are popular with children and young people to help parents make informed decisions

(Further websites are available. The ones listed were correct at time of release September 2019)

Staff training opportunities
It is important that staff are kept up-to-date with online safety issues for children and young people but also for them to consider their online presence.

Training is available through the Education and Skills team (NYCC) and the team has a trained CEOP ambassador (there is a cost for this training):

- NYCC Online safety in schools: meeting your statutory safeguarding duties training runs once an academic year
- A twilight/ staff training day version of this NYCC training can be delivered in a school / to a cluster of schools for staff and/ or governor training which can also be purchased alongside an awareness session for parents / carers. There is also a bespoke Early Years / Settings training

To book the following NYCC provided training through North Yorkshire Education Services

- CEOP provide e-learning and face-to-face training events. They only train DBS (or equivalent) cleared professionals who once trained will be provided with a range of training materials to deliver the training to other professionals and / or parents. There is a cost for this training

- Saferinternet provide a range of free online safety training session across the Country

- Mind Ed – provide free online training focused on:
    - Online Risk And Resilience
    - Digital Media and Young People
    - Children and Young People's Digital Lives

- An online safety INSET free presentation developed by childnet has been designed to be delivered by the online safety Lead, or designated staff member, in a school, organisation or child care setting to other professionals. They do also have a presentation that can be delivered to parents.

- NSPCC- Keeping children safe online is a 4 hour online course, £35 per person
    - how children use the internet and technology
    - the risks they face from other people - both other children and adult offenders
    - behaviour by children that exposes them to greater risks online
    - what to do if children experience issues such as cyber bullying or grooming
    - how to make organisations safer places for children to go online
    - how to conduct an e-safety audit and create an acceptable use policy for your organisation.

Further training provider's may be available. The ones listed were correct at time of release September 2019

Appropriate use of Email

- Digital communications with pupils and parents / carers (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official school systems
- The school's e-mail service should be accessed via the provided web-based interface by default
- Under no circumstances should staff or governors contact pupils, parents/carers or conduct any school business using personal e-mail addresses
- School e-mail is not to be used for personal use

- 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.

Appropriate use of mobile phones

- School mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices and under no circumstances should a pupil or parent/carers be given a member of staffs personal mobile number
- Staff should not be using personal mobile phones in school during working hours when in contact with children
- Visitors will be asked not to use their mobile phone whilst on site and to have them away at all times due to all mobile phones containing a camera
- Pupils should adhere to the rules and guidelines set out in the Behaviour Policy / mobile phone policy regarding mobile phone use in school
- All pupils will be required to put their phone / interactive watch in a lockable container at the start of any PE lesson before pupils start to get changed
- All pupils will be required to put their phones / interactive watches in a lockable container at the start of any exams.

Appropriate use of social networking sites

- 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 and governors should not refer to any member of staff, the governing body, pupils, parents/carers, the school or any other member of the school community on any social networking site or blog in a derogatory way
- Pupils will not be allowed on social networking sites on school equipment that have not been pre-approved whether in school or at home. At home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites
- 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
- 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 as a parent/ carer they have any concerns about anything which happens in schools then they will be asked to contact the school directly
- 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. Further guidance and information on this has been developed by Kent County Council which provides useful steps to follow
- Pupils will be taught about online safety when using social networking sites.

Appropriate use of digital images

- The school record of parental permissions granted/not granted must be adhered to when taking images of pupils.

- Under no circumstances should images be taken by staff or governors using privately owned equipment
- Permission to use images of all staff and governors 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
- Schools need to decide if parents/ carers can take images from a school event e.g school play, sports day and how those images can be used, as some parents may object to images of their children being on social networking sites. Schools could decide that parents/ carers need to sign an agreement that they will not share photographs taken at school event through any public median or other schools have decided that the school only will take official photographs taken from the event that parent/ carers could then access. This decision needs to be clearly communicated to all parents/ carers and the reasons behind the decision.
- Schools and settings will liaise with external providers and places visited on school trips to ensure they do not take photographs and use the images on their website / social media without permission of a member of staff from the school.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. For example the school may have an active website and Twitter/ Facebook account / blog which are used to inform, publicise school events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Only school provided removable devices should be used and they should 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.

Appropriate use of websites

- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches
- Staff will preview any recommended sites before use
- “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/ carers 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. Pupils are also aware that all internet use at school is monitored and logged.

- The school only allows the ICT technician and SLT to access to Internet logs.

Passwords are an important element of keeping the users of the school's ICT systems safe

Use of passwords for staff and governors
- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Use of passwords for pupils
- Should only let school staff know their in-school passwords
- Should not share their password with another pupil / sibling
- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow pupils to change passwords

Use of School ICT Equipment
- 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 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
- All should ensure any screens are locked 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.

Monitoring
All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Schools accessing their internet support from Schools ICT can now access Smoothwall's reporting mechanism which will identify pupils that are searching for websites / using search words that may be inappropriate. It will also highlight issues through the content of the site e.g reference to suicide. Other providers are available.

Incident Reporting
Any online safety incidents must immediately be reported to the designated safeguarding lead if it is a member of staff, pupil or parent/carer who will investigate further following online safety and safeguarding policies and guidance.

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 1 is a table which shows how

many schools currently consider the benefit of using a range of technologies for education purposes against the risks and disadvantages. Listed in Appendix 2 are a range of activities that are unacceptable and / or illegal. Appendix 3 and 4 are some suggested 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 tables should be consulted and liaise with the Police should take place. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence.
The police are also keen for any wider context concerns and concerns within the community that are not child specific these should be submitted to the Police through the Police Partnership intel sharing form http://www.safeguardingchildren.co.uk/professionals/forms-for-professionals

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.

Online safety curriculum for pupils that is age appropriate and is a well-planned and taught curriculum
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

A school needs to provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected to manage and reduce these risks. The online safety policy needs to explain how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

The Government has announced that Relationships and Sex Education and Health Education will become statutory for all schools in September 2020. The final Relationships Education, Relationships and Sex Education and Health Education guidance was published in June 2019.
It is recommended that schools start to plan for these statutory requirements before September 2020 and they are incorporated in the planned PSHE curriculum that many schools are already providing.

The guidance specifically refers to education for all pupils about online safety both as a discrete topic area but also as an integral part of the planned curriculum;

- **In this guidance where topics occur equally on and offline they are accommodated in the core content under the most applicable theme with the assumption that teachers will deliver them in a way that reflects that pupils will be negotiating issues and opportunities in these areas in all contexts, including online. Where there are topics with exclusively online content or implications this is drawn out explicitly.**
- Schools should be aware that for many young people the distinction between the online world and other aspects of life is less marked than for some adults. Young people often

operate very freely in the online world and by secondary school age some are likely to be spending a substantial amount of time online. Where topics and issues outlined in this guidance are likely to be encountered by pupils online, schools should take this into account when planning how to support them in distinguishing between different types of online content and making well-founded decisions.

- More broadly, the internet and social media have other important characteristics which young people should be aware of in order to help them use them discriminatingly. For example, social media users are sometimes prepared to say things in more extreme, unkind or exaggerated ways than they might in face to face situations, and some users present highly exaggerated or idealised profiles of themselves online. Some platforms attract large numbers of users with similar, sometimes extreme, views, who do not welcome dissent or debate. Young people should be aware that certain websites may share personal data about their users, and information collected on their internet use, for commercial purposes (i.e. to enable targeted advertising). In addition, criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. Schools should take these factors into account when planning teaching of these subjects and consider the overlap with their wider curriculum to ensure pupils know how to keep themselves and their personal information safe.

The guidance also sets out that; "**Effective teaching in these subjects will ensure that core knowledge is broken down into units of manageable size and communicated clearly to pupils, in a carefully sequenced way, within a planned programme or lessons.** Teaching will include sufficient well-chosen opportunities and contexts for pupils to practise applying and embedding new knowledge so that it can be used skilfully and confidently in real life situations"

The aspects that schools will have to deliver under the new statutory requirements from September 2020

Topic areas for primary schools – Under each topic heading there are learning outcomes that pupils should know by the end of primary school	**Topic areas for secondary schools** – Under each topic heading there are learning outcomes that pupils should know by the end of secondary school
Relationships Education • Families' and people who care for me • Caring friendships • Respectful relationships • Online relationships • Being safe **Health Education** • Mental wellbeing • Internet safety and harms • Physical health and fitness • Healthy eating • Drugs, alcohol and tobacco • Health and prevention • Basic First Aid • Changing adolescent body (puberty)	**Relationships and Sex Education** • Families • Respectful relationships, including friendships • Online and media • Being Safe • Intimate and sexual relationships including sexual health **Health Education** • Mental Wellbeing • Internet safety and harms • Physical health and fitness • Healthy Eating • Drugs, alcohol and tobacco • Health and prevention • Basic first aid • Changing adolescent body (puberty)

	The law It is important for young people to know what the law says about safeguarding issues. There are many different legal provisions whose purpose is to protect young people and which ensure young people take responsibility for their actions. Pupils should be aware of the relevant legal provisions when relevant topics are being taught for example: • marriage • consent, including the age of consent • violence against women and girls • online behaviours including image and information sharing (including 'sexting, youth produced sexual imagery, nudes etc) • pornography • abortion • sexuality • substance misuse • violence and exploitation by gangs • extremism / radicalisation • criminal exploitation (for example through gang involvement or county lines) • hate crime • female genital mutilation (FGM)

Keeping Children Safe in Education, 2019

Online safety education plays a vital part in schools fulfilling their **statutory duties to protect and safeguard** their pupils. When considering the online safety provision a school needs to be aware of the requirements set out in Keeping children safe in education guidance for schools' which states that schools, "should ensure that children are taught about safeguarding, including online safety".

Ofsted Inspection Framework, 2019

Online safety education can make a contribution to judgments under the Ofsted Common Inspection Framework, particularly in the areas of personal development and safeguarding. Further information on Ofsted expectations in relation to online policy and provision can be found in Appenidx 8 but the Ofsted inspection guidance does refer directly to the incoming statutory requirements for Relationships, Relationships and Sex Education and Health Education

- From September 2019, schools are able to follow a new relationships and sex education and health education curriculum. From September 2020, they will be required by law to follow it. Primary-age children must be taught about positive relationships and respect for others, and how these are linked to promoting good mental health and well-being. In addition, sex education will become mandatory at secondary level.
- **If a school is failing to meet its obligations, inspectors will consider this when reaching the personal development judgement.**

Online safety education should be a planned online safety curriculum 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 and will meet the statutory requirements for schools from September 2020.

Schools can access the **North Yorkshire curriculum entitlement framework for PSHE and Citizenship** which sets out ***suggested learning outcomes for key stages 1-4*** and ***provides links to supporting age appropriate resources which includes online safety*** (there are also named resources to teach about issues that can arise both on and offline such as grooming, child exploitation, pornography, radicalisation and extremism all of which are safeguarding issues).

The Government have published the non-statutory guidance for schools, '**Teaching online safety in school, guidance supporting schools to teach their pupils how to stay safe online within new and existing school subjects** which aims to provide schools with information on the potential harm or risk for young people, what the teaching should be to minimise the risk and where in the curriculum this could be covered. It also signposts to a range of supporting materials.

The government and a range of supporting organisations have produced Education for a Connected World – a Framework to equip children and young people for a digital life (from Early Years upwards)

A useful key document to read is the 'Key principles of effective prevention education' - produced by the PSHE Association on behalf of CEOP. These principles will help PSHE education professionals to teach high-quality online safety education as part of their broader PSHE programmes.

Additional guidance and information on a range of aspects that link to Online Safety and Safeguarding to inform a school's Online Safety Policy and effective provision

Prevent

The use of technologies and accessing information and materials should all be understood and considered in any aspects in relation to Prevent, radicalisation and extremism.

An e-learning package from the Home Office on Prevent is available

The North Yorkshire Safeguarding board has a professional practice guide on Prevent

For further information and links to key documents see: http://cyps.northyorks.gov.uk/prevent

North Yorkshire Community Safety Partnership Working with Individuals Vulnerable to Extremism in Education Settings (Practice Guidance)

Sexting in schools and colleges: responding to incidents and safeguarding young people - UKCCIS Guidance

This is non-statutory, but should be read alongside 'Keeping children safe in education'. This is important guidance and should be read and understood by DSLs, appropriately communicated to the staff team and incorporated into the schools online safety policy.

This is clear guidance to schools about how they should handle incidents where pupils under-18 take and/or share naked images of other under-18s, including themselves. This new guidance takes a safeguarding focus, rather than a simple criminal response, and, in some circumstances, allows schools to deal with incidents without involving the police.

There is no clear definition of 'sexting'. Instead, this document talks about 'youth-produced sexual imagery'. This is imagery that is being created by under 18s themselves and involves still photographs, video, and streaming. In the guidance, this content is described as sexual and not indecent.

Incidents covered by this guidance:

- Person under 18 creates a sexual image of themselves and shares it with another person under 18.
- A person under 18s shares an image of another under 18 with another person under 18 or an adult.
- A person under 18 is in possession of sexual imagery created by another person under 18.

Incidents not covered by this guidance:

- Under 18s sharing adult pornography.
- Under 18s sharing sexual texts without sexual imagery.
- Adults sharing sexual imagery of under 18s. (This is child sexual abuse and must always be reported to police.)

Child Sexual Exploitation (CSE)

The definition of CSE was updated by the government in February 2017, 'Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact; it can also occur through the use of technology:

- can affect any child or young person (male or female) under the age of 18 years, including 16 and 17 year olds who can legally consent to have sex;
- can still be abuse even if the sexual activity appears consensual;
- can include both contact (penetrative and non-penetrative acts) and non-contact sexual activity;
- can take place in person or via technology, or a combination of both;
- can involve force and/or enticement-based methods of compliance and may, or may not, be accompanied by violence or threats of violence;
- may occur without the child or young person's immediate knowledge (through others copying videos or images they have created and posting on social media, for example);
- can be perpetrated by individuals or groups, males or females, and children or adults. The abuse can be a one-off occurrence or a series of incidents over time, and range from opportunistic to complex organised abuse; and
- is typified by some form of power imbalance in favour of those perpetrating the abuse. Whilst age may be the most obvious, this power imbalance can also be due to a range of other factors including gender, sexual identity, cognitive ability, physical strength, status, and access to economic or other resources.

Governments update on Child sexual exploitation is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591903/CSE_Guidance_Core_Document_13.02.2017.pdf

The Local Children's Safeguarding Board has produced a practice guide for professionals and training on CSE available at: http://www.safeguardingchildren.co.uk/professionals/practice-guidance

Sexual violence and sexual harassment between children in schools and colleges (DfE), May 2018 and from Keeping Children Safe in Education

The advice provided by the Department for Education focuses on, child on child sexual violence and sexual harassment at schools and colleges. The advice covers children of all ages, from the primary through secondary stage and into colleges and is referring to the following types of behaviours:

- bullying (including cyberbullying);
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm;
- sexual violence and sexual harassment;
- sexting (also known as youth produced sexual imagery); and
- initiation/hazing type violence and rituals (Hazing is any action taken or any situation created intentionally that causes embarrassment, harassment or ridicule and risks emotional and/or physical harm to members of a group or team, whether new or not, regardless of the person's willingness to participate)

A school needs to ensure their policies include both on and offline peer on peer abuse, sexual violence and harassment and that these behaviours are challenged within a school and that the learning about these behaviours is part of the planned RSE curriculum for pupils including how to get help and support. Cambridge Lets Learn Together service have developed a, Safer Corridor Toolkit' to support secondary schools where leaders wish to develop or review their responses to sexual harassment (there is a cost for this resource).

Upskirting

Upskirting is a highly intrusive practice, which typically involves someone taking a picture under another person's clothing without their knowledge, with the intention of viewing their genitals or buttocks (with or without underwear). It is now illegal. More information can be accessed here

Technology assisted Harmful sexual behaviour

Harmful sexual behaviour (HSB) is developmentally inappropriate sexual behaviour which is displayed by children and young people and which may be harmful or abusive. It may also be referred to as sexually harmful behaviour or sexualised behaviour. It can be displayed towards younger children, peers, older children or adults, and is harmful to the children and young people who display it, as well as the people it is directed towards.

Technology assisted HSB (TA-HSB) is sexualised behaviour which children or young people engage in using the internet or technology such as mobile phones. As with 'offline' HSB, TA-HSB encompasses a range of behaviours including:

- viewing pornography (including extreme pornography or viewing indecent images of children)
- sexting

Brook have devised the 'Traffic Light Tool' to help professionals who work with children and young people to identify, assess and respond appropriately to sexual behaviours. The normative list aims to increase understanding of healthy sexual development and distinguish it from harmful behaviour for different aged children and young people. The traffic light tool and all supporting guidance can be found at www.brook.org.uk/traffic-lights

The Local Children's Safeguarding Board has produced a practice guide for professionals http://www.safeguardingchildren.co.uk/professionals/practice-guidance

NSPCC provides some Online courses (at a cost) to help manage harmful sexual behaviour in primary or secondary schools in the UK

Some further risks children and young people may face include (with signposting to further information and guidance)

- 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.
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying and the Anti-bullying Alliance has a range of CPD modules for professionals including one on cyberbullying as well as supporting resources
- 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 and illegal downloading of music or video files
- Monitoring Screen Time
- Impact of social media on Body Image
- Selling substances over social media
- Information on the Dark web
- Gaming is now an identified disorder
- Information on internet hoaxes, memes and challenges and where to check if information is correct.
- Online platforms are increasingly being used to perpetrate domestic abuse and stalking. there is a range of guidance to support these issues
- Criminal Exploitation North Yorkshire Safeguarding board criminal exploitation and county lines practice guide and County Lines – Children Society Toolkit for professionals

Appendix 1

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows provides examples of different ways the technology can be used. Schools need to consider the benefit of using these technologies for education purposes against the risks and disadvantages. This is for guidance only and your school will need to decide on what is right for your school as for some aspects no 'ticks' have been provided.

	Staff and other adults				**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 but used when in the presence of pupils	✓							
Mobile phones used in lessons				✓			e.g taking a photo of some work for revision purposes	
Use of mobile phones in social time needs to be explicit in the mobile phone policy	✓							
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	✓ (within the AUP)				✓ (within the AUP)			

use									
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		✓				✓			

When using communication technologies the school considers the following as good practice:

- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the school policy) the receipt of any email/ message via technology that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, governors and pupils or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff and governors

Appendix 2
Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
Possession of an extreme pornographic image (grossly offensive, disgusting or					✓

otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
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			✓		

The police are keen for any wider context concerns and concerns within the community that are not child specific these should be submitted to the Police through the Police Partnership intel sharing form
http://www.safeguardingchildren.co.uk/professionals/forms-for-professionals

Appendix 3
Incidents Involving pupils and action 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 DSL**	**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 4
Incidents involving members of staff and action taken

Incidents involving members of staff	**Refer to the Headteacher** ***See below**	**Refer to technical support staff for action re filtering, security etc**	**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 / governors 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	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓	✓
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.

Appendix 5

Model 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 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 6
Model Acceptable Internet Use Policy – adults who work in the school community (this includes governors and volunteers)

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

This policy is intended to ensure that:

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

The school will try to ensure that staff, governors and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff, governors and volunteers to agree to be responsible users.

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 unless accessing a secure online platform specifically provided by the school
- I will not store any school data (in line with the schools data protection policy) on personal devices
- 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
- *For Governors I will not add new families as social media contacts whilst a governor*
- I will not 'discuss' any school issues on social media. *For governors this is covered in the Governors code of conduct*
- 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, governor 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 7

Home- school agreement OR Acceptable Internet Use Policy Parents / Carers

The following could be include in a home – school agreement form that many schools already have in place

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The Internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. However, the use of these new technologies can put young people at risk within and outside the school. All users have an entitlement to safe Internet access at all times.

To support parents / carers in learning about the online risks, support you to be able to talk to your children the risks and learn how to set up parental controls there is a section on our school website signposting you to range of supporting websites.

As a parent / carer of a child at this school we are asking that:

- You will contact school and all members of staff within school through the appropriate school communication channels and treat everyone with respect and professionalism. You will not contact any member of staff through a personal email address or phone number
- You will not ask any member of school staff to 'be-friend' you on a social networking site as all staff have been requested not to accept any 'friend' offers
- Ensure you 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 you have any concerns about anything which happens in schools then please contact the school directly
- Ensure that any school technology that is brought home by your child is used appropriately for school based work and that where available your home internet provider will have parental controls set that minimise the risk of your child accessing anything inappropriate online
- Ensuring that school equipment is only used by the pupil who the equipment has been provided for and no other family member, sibling or friends use the equipment
- Ensure that you have signed the photograph permission form which sets out that parent/ carers *are unable to take photographs/films at schools events and can only access the official photographs taken by the school which cannot be shared on any public accessed social networking site / website OR any photographs/films that are taken of school events will not be shared on any publically accessed social networking site or website*

Appendix 8
Ofsted Inspection Framework September 2019

The new Ofsted Framework (September 2019) has a personal development judgement and the guidance states, “The personal development judgement evaluates the school’s intent to provide for the personal development of all pupils, and the quality with which the school implements this work”. This judgement will focus on a range of aspects. The following aspects are ones that could be directly linked to the effective provision of online safety:

- developing responsible, respectful and active citizens who are able to play their part and become actively involved in public life as adults
- developing pupils’ character, which we define as a set of positive personal traits, dispositions and virtues that informs their motivation and guides their conduct so that they reflect wisely, learn eagerly, behave with integrity and cooperate consistently well with others. This gives pupils the qualities they need to flourish in our society
- developing pupils’ confidence, resilience and knowledge so that they can keep themselves mentally healthy
- enabling pupils to recognise online and offline risks to their well-being – for example, risks from criminal and sexual exploitation, domestic abuse, female genital mutilation, forced marriage, substance misuse, gang activity, radicalisation and extremism – and making them aware of the support available to them
- enabling pupils to recognise the dangers of inappropriate use of mobile technology and social media
- developing pupils’ age-appropriate understanding of healthy relationships through appropriate relationship and sex education

The Ofsted inspection guidance does refer directly to the incoming statutory requirements for Relationships, Relationships and Sex Education and Health Education

- From September 2019, schools are able to follow a new relationships and sex education and health education curriculum. From September 2020, they will be required by law to follow it. Primary-age children must be taught about positive relationships and respect for others, and how these are linked to promoting good mental health and well-being. In addition, sex education will become mandatory at secondary level.
- **If a school is failing to meet its obligations, inspectors will consider this when reaching the personal development judgement.**

Ofsted, Inspecting safeguarding in early years, education and skills settings (September 2019) has a number of aspects that could relate to effective online safety eductaion provision :

- Action is taken to ensure that children are taught about safeguarding risks, including online risks
- As part of the curriculum, children and learners are supported to understand what constitutes a healthy relationship both online and offline, and to recognise risk, for example risks associated with criminal and sexual exploitation, domestic abuse, female genital mutilation, forced marriage, substance misuse, gang activity, radicalisation and extremism, and are aware of the support available to them
- Staff, leaders and managers understand the risks posed by adults or young people who use the internet to bully, groom or abuse children, learners and vulnerable adults; there are well-developed strategies in place to keep learners safe and to support them in learning how to recognise when they are at risk and how to get help when they need it
- Children and learners are protected and know how to get support if they experience bullying, homophobic behaviour, racism, sexism and other forms of discrimination. Any

discriminatory behaviours are challenged and help and support are given to children about how to treat others with respect.

- Adults understand the risks associated with using technology, including social media, of bullying, grooming, exploiting, radicalising or abusing children or learners. They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe.
- Inspectors will evaluate, where applicable, the extent to which the provision is successfully promoting and supporting children's and learners' safety. Inspectors will consider, among other things, children's and learners' understanding of healthy and unhealthy relationships and how they are supported to keep themselves safe from relevant risks such as exploitation and extremism, including when using the internet and social media. Inspectors should include online safety in their discussions with children and learners (covering topics such as online bullying and safe use of the internet and social media). Inspectors should investigate what the school or further education and skills provider does to educate pupils in online safety and how the provider or school deals with issues when they arise.
- In relation to early years, inspectors should consider how staff promote young children's understanding of how to keep themselves safe from relevant risks and how this is monitored across the provision.