ELSTON HALL
Multi-Academy Trust

Remote and Online Learning Policy

Policy created / reviewed by:	Mrs R Wood
Approved by:	Mrs L Dollery
Approved on:	January 2021
Next Review due:	January 2022

Introduction

Research suggests that online learning has been shown to increase retention of information, and take less time, meaning the changes coronavirus have caused might be here to stay. Most schools have always had some element of online learning in place however, schools will all be at varying stages of development.

Learning online has countless benefits. Certainly, during the COVID-19 crisis the importance of online learning has been brought to the forefront of education thinking. The implementation of online learning enables a school to work more closely with parents and their community to provide a blended learning approach combining online educational learning with traditional classroom methods. This enables the transfer of learning from school to home and vice versa.

We will look at Remote Learning in two aspects:
-Online Learning in School
-Remote Learning at Home

Remote Teaching

Schools in the Elston Hall Multi Academy Trust provide a range of educational programmes which can be accessed via the school website, Class Do Jo's, Trust Learning Platform (www.ehlt.org.uk), along with lessons which are emailed directly to pupils. These are accessed online through our secure portal using the school website and Learning Platform. This transfers the school's usual procedures for lesson planning, teaching and feedback to an online environment. Work can be completed by our pupils online using One Note or through a range of online educational programmes, which can be accessed via the school website.

Schools in the Elston Hall Multi Academy Trust provide a range of educational programmes. We are currently developing our Trust Learning Platform (www.ehlt.org.uk), which will allow families to access remote learning through a secure portal. This transfers the school's usual procedures for lesson planning, teaching and feedback to an online environment. Work can be completed by our pupils online using One Note or through a range of online educational programmes. While this Platform is currently in use at Pheasey Park Primary School, remaining Trust schools send remote learning directly to parents via email (Elston Hall Primary School, Palmers Cross Primary School and Edward the Elder Primary School) or Class Dojos (Goldthorn Park Primary School).

Today's children are citizens of a digital world. In their daily lives the use of the internet and digital technologies represents a seamless extension of the physical world. Their emotional lives and their development are bound up in the use of these technologies. In contrast to many adults for whom these technologies are additional tools to be used for specific tasks, many of today's children do not even notice they are using these technologies. As online content, social networking 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.

Aims:

- Ensure provision is in place so that all pupils have access to high quality learning resources.
- Protect pupils from the risks associated with using devices connected to the internet.
- Minimise the disruption to pupils' education and the delivery of the curriculum
- Ensure staff, parent, and pupil data remains secure and is not lost or misused.
- Ensure robust safeguarding measures continue to be in effect during the period of remote learning.
- Ensure all pupils have the provision they need to complete their work to the best of their ability, and to remain happy, healthy, and supported during periods of remote learning.
- Ensure continuity of learning between home and school including during periods of lockdown and pupil absence.

Online Safety

The Internet is a fantastic resource that children are using as a normal part of everyday life. However, in the same way that we do not allow them to wander around the world by themselves or talk to strangers, it is equally important that we protect them when they are exploring the virtual world. During ICT lessons and class discussions children are informed about keeping safe online.

Online Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets and computers as well as collaboration tools and personal publishing. It 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 experience. We need to equip children with the knowledge to navigate the online world safely.

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to the following:

Equality Act 2010
Education Act 2004
The General Data Protection Regulation (GDPR)
Data Protection Act 2018

This policy has due regard to national guidance including, but not limited to, the following:
DfE (2020) 'Keeping children safe in education'
DfE (2019) 'School attendance'
DfE (2017) 'Special educational needs and disability code of practice: 0 to 25 years'
DfE (2018) 'Health and safety: responsibilities and duties for schools'
DfE (2018) 'Health and safety for school children'
DfE (2016) 'Children missing education'

This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Data Protection Policy
- Special Educational Needs and Disabilities (SEND) Policy
- Behaviour for learning Policy
- Accessibility Policy
- Marking and Feedback Policy
- Curriculum Policy
- Assessment Policy

- Online Safety Policy and Protocols
- Health and Safety Policy
- Attendance Policy
- ICT Acceptable Use Policy
- Staff Code of Conduct
- GDPR Plan
- Children Missing Education Policy

Keeping Children Safe in Education

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. 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.

School Procedures

- The ICT Leader is the appointed person to co-ordinate Online Safety.
- The Remote Learning and Online Safety Policy has been agreed by senior management and approved by governors.
- The Online Safety Policy and Protocols and its implementation will be reviewed annually.
- Ongoing staff Online Safety training (making staff aware of the different social networks and the appropriate terminology.
- Use of CEOP (Child Exploitation and Online Protection Centre) as an online reporting mechanism.
- Online Safety is covered in staff meetings, parent workshops, ICT lessons and assemblies.
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Roles and Responsibilities:

The Governing Body is responsible for:

- Ensuring that the school has robust risk management procedures in place.
- Ensuring that the school has a business continuity plan in place, where required.
- Evaluating the effectiveness of the school's remote learning arrangements.

The Head of School is responsible for:

- Ensuring that staff, parents and pupils adhere to the relevant policies at all times.
- Ensuring that there are arrangements in place for identifying, evaluating, and managing the risks associated with remote learning.
- Ensuring that there are arrangements in place for monitoring incidents associated with remote learning.
- Overseeing that the school has the resources necessary to action the procedures in this policy.

- Reviewing the effectiveness of this policy on an annual basis and communicating any changes to staff, parents, and pupils.
- Arranging any additional training staff may require to support pupils during the period of remote learning.
- Conducting reviews on a regular basis of the remote learning arrangements to ensure pupils' education does not suffer.

The Health and Safety Officer is responsible for:

- Ensuring that the relevant health and safety risk assessments are carried out within the agreed timeframes, in collaboration with the **Head of School**.
- Putting procedures and safe systems of learning into practice, which are designed to eliminate or reduce the risks associated with remote learning.
- Ensuring that pupils identified as being at risk are provided with necessary information and instruction, as required.
- Managing the effectiveness of health and safety measures through a robust system of reporting, investigating, and recording incidents.

The DPO is responsible for:

- Overseeing that all school-owned electronic devices used for remote learning have adequate anti-virus software and malware protection.
- Ensuring all staff, parents, and pupils are aware of the data protection principles outlined in the GDPR.
- Ensuring that all computer programs used for remote learning are compliant with the GDPR and the Data Protection Act 2018.
- Overseeing that any ICT equipment used for remote learning is resilient and can efficiently recover lost data.

The DSL and Online Safety Leads are responsible for:

- Attending and arranging, where necessary, any safeguarding meetings that occur during the remote learning period.
- Liaising with the **ICT technicians** to ensure that all technology used for remote learning is suitable for its purpose and will protect pupils online.
- Identifying vulnerable pupils who may be at risk if they are learning remotely.
- Ensuring that child protection plans are enforced while the pupil is learning remotely, and liaising with the **Head of School** and other organisations to make alternate arrangements for pupils who are at a high risk, where required.
- Identifying the level of support or intervention required while pupils learn remotely and ensuring appropriate measures are in place.
- Liaising with relevant individuals to ensure vulnerable pupils receive the support required during the period of remote working Ensuring all safeguarding incidents are adequately recorded and reported.

The SENCO is responsible for:

- Liaising with the **ICT technicians** to ensure that the technology used for remote learning is accessible to all pupils and that reasonable adjustments are made where required.

- Ensuring that pupils with EHC plans continue to have their needs met while learning remotely, and liaising with the **Head of School** and other organisations to make any alternate arrangements for pupils with EHC plans and IHPs.
- Identifying the level of support or intervention that is required while pupils with SEND learn remotely.
- Ensuring that the provision put in place for pupils with SEND is monitored for effectiveness throughout the duration of the remote learning period.

The ICT Technicians are responsible for:

- Ensuring that all school-owned devices used for remote learning have suitable anti-virus software installed, have a secure connection, can recover lost work, and allow for audio and visual material to be recorded, where required.
- Ensuring that any programs or networks used for remote learning can effectively support a large number of users at one time, where required, e.g. undertaking 'stress' testing.
- Working with the **SENCO** to ensure that the equipment and technology used for learning remotely is accessible to all pupils and staff.

Staff Members are Responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Reporting any health and safety incidents to the health and safety officer and asking for guidance as appropriate.
- Reporting any safeguarding incidents to the **DSL/Online Safety Lead** and asking for guidance as appropriate.
- Taking part in any training conducted to meet the requirements of this policy, including training on how to use the necessary electronic equipment and software.
- Reporting any dangers or potential dangers they identify, as well as any concerns they may have about remote learning, to the **Head of School**.
- Reporting any defects on school-owned equipment used for remote learning to an ICT technician.
- Adhering to the Staff Code of Conduct at all times.

Parents are responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring their child is available to learn remotely at the times set out in this policy, and that the schoolwork set is completed on time and to the best of their child's ability.
- Reporting any technical issues to the school as soon as possible.
- Ensuring that their child always has access to remote learning material during the times set out in this policy.
- Reporting any absence in line with the terms set out in this policy and the school's attendance policy.
- Ensuring their child uses the equipment and technology used for remote learning as intended.
- Adhering to the **Parent Code of Conduct** at all times.

Pupils are Responsible for:

- Adhering to this policy at all times during periods of remote learning.
- Ensuring they are available to learn remotely at the times set out in this policy, and that their schoolwork is completed on time and to the best of their ability.
- Reporting any technical issues to **their teacher** as soon as possible.

- Ensuring they have access to remote learning material and notifying a responsible adult if they do not have access.
- Notifying a responsible adult if they are feeling unwell or are unable to complete the schoolwork they have been set.
- Ensuring they use any equipment and technology for remote learning as intended.
- Adhering to the **Behaviour for Learning Policy** at all times.

Resources

The school will accept a range of different teaching methods during remote learning to help explain concepts and address misconceptions easily. For the purpose of providing remote learning, the school may make use of:

- Learning Platform (www.ehlt.org.uk)
- School website
- Work booklets
- Email
- Past and mock exam papers
- Current online learning portals
- Online educational programmes **(listed on school websites)*
- Reading tasks
- Live webinars
- Pre-recorded video or audio lessons
- TEAMS

- Teachers will review the DfE's list of online education resources and utilise these tools as necessary, in addition to existing resources.
- When providing remote learning for a class bubble closure or national lockdown, teachers must be available between 8:30am and 3:30pm (unless they are unwell themselves).
- When providing remote learning for a pupil/small group of pupils who are self-isolating, teachers will be available in working hours when they are not teaching i.e. 8-9am, lunch 12-1 and 3.30-5pm.
- If they are unable to work for any reason during this time, for an example due to sickness or caring for a dependent, they should report this using the normal absence procedures.
- Reasonable adjustments will be made to ensure that all pupils have access to the resources needed for effective remote learning.
- Teachers will ensure the software chosen for online learning have a range of accessibility features, e.g. voice-to-text conversion, to support pupils with SEND.
- Lesson plans will be adapted to ensure that the curriculum remains fully accessible and inclusive via remote learning.
- The school will review the resources pupils have access to and adapt learning to account for all pupils needs by using a range of different formats, e.g. providing work on PDFs which can easily be printed from a mobile device.
- Work packs will be made available for pupils who do not have access to a printer – these packs can be collected from school.
- Teaching staff will liaise with the **SENCO** and other relevant members of staff to ensure all pupils remain fully supported for the duration of the remote learning period.
- The **SENCO** will arrange additional support for pupils with SEND which will be unique to the individual's needs, e.g. via weekly phone calls.

- Any issues with remote learning resources will be reported as soon as possible to the relevant member of staff.
- Pupils will be required to use their own or family-owned equipment to access remote learning resources, unless the school agrees to provide or loan equipment, e.g. laptops.
- Pupils and parents will be required to maintain the upkeep of any loaned equipment they use to access remote learning resources.
- Teaching staff will oversee academic progression for the duration of the remote learning period and will mark and provide feedback on work.
- The arrangements for any 'live' classes, e.g. webinars, will be communicated via **email** and announcements on website/class sites no later than **one day** before the agreed time and kept to a reasonable length of no more than **one hour** per session.
- The **ICT Technicians** are not responsible for providing technical support for equipment that is not owned by the school.

Costs and Expenses:

The school will not contribute to any household expenses incurred while pupils learn remotely, e.g. heating, lighting, or council tax.

The school will not reimburse any costs for travel between pupils' homes and the school premises.

The school will not reimburse any costs for childcare.

If a pupil is provided with school-owned equipment, the pupil and their parent will sign and adhere to the **Acceptable Use Agreement** prior to commencing remote learning.

Free school Meals will be organised for eligible families.

Online Safety

Video Communication:

All staff and pupils using video communication must:

- Communicate in groups or with an adult present – one-to-one sessions are not permitted.
- Wear suitable clothing – this includes others in their household.
- Be situated in a suitable 'public' living area within the home with an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication.
- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute video material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.
- Always remain aware that they are visible.

Audio Communication:

All staff and pupils using audio communication must:

- Use appropriate language – this includes others in their household.
- Maintain the standard of behaviour expected in school.
- Use the necessary equipment and computer programs as intended.
- Not record, store, or distribute audio material without permission.
- Ensure they have a stable connection to avoid disruption to lessons.

- Always remain aware that they can be heard.

The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the **SLT**, in collaboration with the **SENCO**.
Pupils not using devices or software as intended will be disciplined in line with the **Behaviour for Learning Policy**.
The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.
The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.
The school will communicate to parents via telephone about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites and pop ups.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Safeguarding

This section of the policy will be enacted in conjunction with the school's **Child Protection and Safeguarding Policy**, which has been updated to include safeguarding procedures in relation to remote working.

The **DSL** and **Head of School** will identify 'vulnerable' pupils (pupils who are deemed to be vulnerable or are at risk of harm) via risk assessment prior to the period of remote learning. In the case of a Local/National Lockdown, vulnerable pupils will be invited to attend school alongside children of critical workers.
The **DSL** will arrange for regular contact to be made with vulnerable pupils not attending school, prior to the period of remote learning.
Phone calls made to vulnerable pupils will be made using school phones where possible.

The **DSL** will arrange for regular contact with vulnerable pupils **once** per **week** at minimum, with additional contact, including home visits, arranged where required.

All contact with vulnerable pupils will be recorded.
The **DSL** will keep in contact with vulnerable pupils' social workers or other care professionals during the period of remote working, as required.

All home visits **must**:

- Have at least **one** suitably trained individual present.
- Be undertaken by no fewer than **two** members of staff.
- Be suitably recorded on paper and the records stored so that the **DSL** has access to them.
- Actively involve the pupil.

Vulnerable pupils will be provided with a means of contacting the school for support via the Learning Platform.
The **DSL** will meet (in person or remotely) with the relevant members of staff to discuss new and current safeguarding arrangements for vulnerable pupils learning remotely.
All members of staff will report any safeguarding concerns to the **DSL** immediately.
Pupils and their parents will be encouraged to contact the **DSL** if they wish to report safeguarding concerns, e.g. regarding harmful or upsetting content or incidents of online bullying. The school will also signpost families to the practical support that is available for reporting these concerns.

Data Protection:

This section of the policy will be enacted in conjunction with the school's **Data Protection Policy**.
Staff members will be responsible for adhering to the GDPR when teaching remotely and will ensure the confidentiality and integrity of their devices at all times.

Sensitive data will only be transferred between devices if it is necessary to do so for the purpose of remote learning and teaching.
Any data that is transferred between devices will be suitably encrypted or have other data protection measures in place so that if the data is lost, stolen, or subject to unauthorised access, it remains safe until recovered.
Parents' and pupils' up-to-date contact details will be collected prior to the period of remote learning.
All contact details will be stored in line with the **Data Protection Policy** and retained in line with the **Records Management Policy**.
The school will not permit paper copies of contact details to be taken off the school premises.
Pupils are not permitted to let their family members or friends use any school-owned equipment which contains personal data.
Any breach of confidentiality will be dealt with in accordance with the school's **Data and GDPR Plan**.
Any intentional breach of confidentiality will be dealt with in accordance with the school's **Behaviour for Learning Policy**.

Marking and Feedback:

All schoolwork completed through remote learning must be:

- Finished when returned to the relevant member of teaching staff.
- Returned on or before the deadline set by the relevant member of teaching staff.
- Completed to the best of the pupil's ability.

- The pupil's own work.
- Marked in line with the **Marking and Feedback Policy**.
- Returned to the pupil, once marked, by an agreed date.

The school expects pupils and staff to maintain a good work ethic during the period of remote learning.
Pupils are accountable for the completion of their own schoolwork – teaching staff will contact parents via **email** if their child is not completing their schoolwork or their standard of work has noticeably decreased.
Teaching staff will monitor the academic progress of pupils with and without access to the online learning resources and discuss additional support or provision with the **Head of School** as soon as possible. Teaching staff will monitor the academic progress of pupils with SEND and discuss additional support or provision with the **SENCO** as soon as possible.
The school accepts a variety of formative assessment and feedback methods, e.g. through quizzes and other digital tools from teachers, and will support them with implementing these measures for remote learning where possible.

Health and Safety:

This section of the policy will be enacted in conjunction with the school's **Health and Safety Policy**.

Teaching staff and **ICT technicians** will ensure pupils are shown how to use the necessary equipment and technology safely and correctly prior to the period of remote learning.
If using electronic devices during remote learning, pupils will be encouraged to take a **five-minute** screen break every **two hours**.
Screen break frequency will be adjusted to **five minutes** every **hour** for younger pupils or pupils with medical conditions who require more frequent screen breaks.
If any incidents or near-misses occur in a pupil's home, they or their parents are required to report these to the **health and safety officer** or other relevant member of staff immediately so that appropriate action can be taken.

School Day and Absence

Pupils are expected to do schoolwork during school day times, although allowances are made for working families who may choose to complete work at different times.
Pupils with SEND or additional medical conditions who require more regular breaks, e.g. sensory breaks, are not expected to do schoolwork during their breaks.
Pupils who are unwell are not expected to be present for remote working until they are well enough to do so.
Parents will inform their **child's teacher** if their child is unwell.
The school will monitor absence and lateness in line with the **Attendance Policy**.

Communication:

The school will ensure adequate channels of communication are arranged in the event of an emergency.
The school will communicate with parents via **letter** and via the **school website** about remote learning arrangements as soon as possible.

The **Head of School** will communicate with staff as soon as possible via **email or telephone** about any remote learning arrangements.

Members of staff involved in remote teaching will ensure they have a working mobile device that is available to take phone calls during their agreed working hours.

The school understands that pupils learning remotely have the right to privacy out-of-hours and should be able to separate their school and home lives – communication is only expected during school hours.

Members of staff will have contact with their line manager at least **once** per **week**.

As much as possible, all communication with pupils and their parents will take place within the school hours.

Parents and pupils will inform the relevant member of staff as soon as possible if schoolwork cannot be completed.

Issues with remote learning or data protection will be communicated to the **pupils' teacher** as soon as possible so they can investigate and resolve the issue.

The **pupils' teacher** will keep parents and pupils informed of any changes to the remote learning arrangements or the schoolwork set.

The **Head of School** will review the effectiveness of communication on a **weekly** basis and ensure measures are put in place to address gaps or weaknesses in communication.

Monitoring and review

This policy will be reviewed on an **annual** basis by the **Head of School**.

Any changes to this policy will be communicated to all members of staff and other stakeholders.

Online learning is an item on the SLT agenda.

Key focus during this meeting entail:

- Discussions on current Online Safety issues or threats.
- Reviewing of policies and procedures.
- Evaluation of teaching of online safety.
- Discussions on emerging technologies.

Managing Information Systems

How will information systems security be maintained?

- The security of the school information systems, systems capacity, security and users will be reviewed regularly.
- The school uses broadband with firewall and filters.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Head teacher and external agencies.
- Personal data sent over the Internet or taken off site will be encrypted. USB pens and external hard drive devices will be password protected.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT Leader will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.
- Internet filtering is conducted by Wolverhampton City Council which logs any misuse by any person accessing school internet sites.

How will E-mail be managed?

- The school uses a secure E-mail system.
- Pupils will not be allowed to access personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- School e-mail will be used for classes communicating outside of the school to another school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers through the office staff.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Emails sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.
- Professional E-mail communication needs to be restricted to only necessary communication.
- An agreed signature format and disclaimer must be added to all staff email accounts.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website and Learning Platform will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Photographs or videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified, unless specified otherwise.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published on the internet. (Website, Learning Platform or External agencies.)
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures.

How will social networking, social media and personal publishing be managed?

- The school will control access by blocking access to social media and social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils
- 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, email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with pupils as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will follow the guidelines when using Social Media tools in the classroom.

- Staff official blogs should be password protected and run from the school website with approval from SLT. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupils use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's Acceptable Use Policy and staff code of conduct.

How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with the Schools Broadband team to ensure that the filtering policy is continually reviewed and improved.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School Online Safety Co-ordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from SLT.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from external agencies.
- Video conferencing should be supervised appropriately for the pupils' age. Pupils should not answer or make a video conference call.

How are emerging technologies managed?

- 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 in formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Policy.
- Video Conferencing will be appropriately supervised for the pupils' age.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to GDPR regulations.

How will Internet access be authorised?

- All staff will be given the School Online Safety Policy and its importance explained.
- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Acceptable ICT Use Agreement' before using any school Education Technology resources.
- The Head of School will ensure that the Remote Learning and Online Safety Policy is implemented and compliance with the policy monitored.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of Internet misuse will be dealt with by the Head of School or a senior member of staff.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Advice on Online Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school who require access to the school's network or internet access will be asked to read and sign an Acceptable Use Policy.
- Pupils' access to the Internet will be under adult supervision.
- Online Safety rules will be displayed where appropriate and discussed with the pupils during ICT lessons and in assemblies.
- Pupils will be informed that network and Internet use will be monitored.
- Parent's attention will be drawn to the School Online Safety Policy in newsletters, Online Safety booklet and on the School website.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- Pupils access will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will 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. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school can accept liability for the material accessed, or any consequences of Internet access
- The school will audit Education Technology use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.
- 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.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.)
- The Online Safety Coordinator will record all reported incidents and actions taken in the School online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school Behaviour Policy and Safeguarding Policies.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or Online Safety officer and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County Online Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the local Online Safety officer.

How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the usual School's complaints procedure.
- Any complaint about staff misuse will be referred to the Head of School.
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Pupils Use of Personal Devices

- Only under exceptional circumstances will Pupil's mobile phones be allowed to be kept in the school office. (e.g. A pupil who uses public transport and needs a phone for safety during the journey, will be able to store the phone in the School Office throughout the day.)
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity unless authorised by SLT.
- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of SLT in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by SLT.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Communication Policy

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- Staff who manage filtering systems or monitor technology use will be supervised by SLT and have clear procedures for reporting issues.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

How will parents' support be enlisted?

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus, the school website and ICT parent workshops.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting Online Safety at other attended events e.g. parent evenings and sports days.

- Parents will be requested to sign an On Line Safety/Internet agreement as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.
  Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the "Online Safety Contacts and References section".
- Tips for parents regarding internet safety are included on the website.