Northern Lights Learning Trust
Hart Primary School Primary School

Online Safety Policy

'To give all the opportunity to be the best that they can be and have fullness of life.'

Prepared by: Jade Tillson (Assistant Headteacher and Computing Lead)
Approved: NLLT Board and Local Governing Body
Signature Chair Local Governing Body:
Date of Renewal: Autumn 2027

Contents

1. Statement of intent
    1.1 Teaching and Learning
2. Scope of the policy
    2.1 Legislation and Guidance
3. Roles and responsibilities
    3.1 Governors and Trust board
    3.2 Head teacher and members of SLT
    3.3 Computing Lead
    3.4 Trust IT Manager
    3.5 Teaching and Support Staff
    3.6 Pupils
    3.7 Parents/Carers
    3.8 Visitors and members of the community
4. Policy Statements
    4.1 Educating pupils about online safety
    4.2 Educating parents about online safety
    4.3 Staff
    4.4 Training – Governors
5 Technical
    5.1 Infrastructure/equipment, filtering, and monitoring
    5.2 Responsibilities for filtering and monitoring
    5.3 Mobile Technologies (including BYOD/BYOT)
    5.4 Use of digital and video images
6. Data Protection
7 Social Media
    7.1 Protecting Professional Identity
    7.2 Personal Accounts
    7.3 Monitoring of Public Social Media
    7.4 Unsuitable/inappropriate activities
8. Responding to incidents of misuse
9. Appendices

1. Statement of intent

Online safety involves internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children about the benefits and risks of using new technology and provides awareness for users to enable them to stay safe and control their online experiences.

The school's online safety policy will operate in conjunction with other policies, including:

- Keeping children safe in education 2026 (KCSIE)
- Child Protection Policy
- Behaviour Policy
- Data Protection Policy
- Child On Child Abuse Policy
- Acceptable Use Policy

1.1 Teaching and Learning

Why internet use is important

- The internet is an essential element in 21st century life for education, business, and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and is a necessary tool for staff and pupils.

Internet use will enhance learning

- The school's internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives and guidelines for internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Internet access will be planned to enrich and extend learning activities.

Pupils will be taught how to evaluate internet content

- Internet derived materials by staff and by pupils must comply with copyright laws.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of every subject.
- Pupils will be taught how to report unpleasant internet content.

2. Scope of the policy

This policy applies to all members of Hart Primary School, including staff, supply workers, pupils, volunteers and apprentices, and visitors who have access and are users of school ICT systems both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers to such an 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 Education Act of 2011 increased these powers regarding searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered in the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform relevant parties of incidents of inappropriate online behaviour that take place out of school.

Schools in England and Wales are required “to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.” (Revised prevent Duty Guidance for England and Wales).

The DfE published revised guidance for “Keeping Children Safe in Education” in September 2021 for school and colleges in England. Included in the revisions, schools are obligated to “ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or college IT system”. However, schools will need to “be careful that ‘over blocking’ does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

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

KCSIE (Para 163 – updated July 2026):
Content: - being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,

- Contact: being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct: behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- Commerce: risks such as gambling, inappropriate advertising, phishing and financial scams

Schools in England are subject to increased scrutiny of online safety through inspection, and the Counter Terrorism and Security Act 2015 requires schools to protect learners from terrorist and extremist material online.

2.1 Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe In Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Generative artificial intelligence (AI) in education - GOV.UK
- Using AI in education settings: support materials - GOV.UK
- Mobile phones in schools - GOV.UK

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

3.1 Governors and Trust board

The Local Governing Body and Trust board are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. They should "ensure online safety is a running and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement." (KCSIE 2026, 166).

The Local Governing Body and Trust board should be doing all that they reasonably can to limit children's exposure to the above risks from the school's system. This

includes ensuring the school has an appropriate filtering and monitoring system in place and ensure a review of their effectiveness is carried out at least once every academic year. The Local Governing Body and Trust board should consider the number and age range of the children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks. This system will be informed in part by the risk assessment required by the Prevent Duty. (KCSIE 2026, 174).

The Local Governing Body and Trust board should be ensuring mobile-phone free expectations are implemented consistently.

3.2 Headteacher/Head of School and members of SLT

The Headteacher/Head of School has a duty of care for ensuring the safety including online safety of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Office Manager and Computing Lead.

The Headteacher/Head of School and the SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made.

The Headteacher/head of School and SLT are responsible for ensuring the Computing Lead and other relevant staff receive sufficient training to enable them to carry out other roles.

3.3 Computing Lead

The Computing Lead will:

- Take day to day responsibilities for online safety issues and has a lead role in establishing and reviewing the school online safety procedures.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provide advice and training for staff
- Liaise with school technical staff
- Use reports of online safety incidents to inform future online safety developments and report to SLT
- Meet with governors (when necessary) to discuss issues, review incident logs and filter logs.
- The Computing Lead elects and supports pupil Digital Leaders to support in the leading of technology and computing.

3.4 Trust IT Manager

The Trust IT Manager - Central IT Team (ithelpdesk@nllt.co.uk) - and other technical support staff (including external stakeholders) are responsible for:

- The school's technical infrastructure is, as far as possible, secure, and not open to misuse or malicious attack.
- That the school meet required online safety technical requirements and any academy guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection procedures, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis and that the implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network, internet, remote access, e mail is regularly monitored in order that any misuse or attempted misuse can be reported to relevant people for investigation.

3.5 Teaching and Support Staff

Teaching and Support Staff (including contractors, ITT students, agency staff and volunteers) are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy.
- They have read, understood, and signed the Acceptable Use Policy.
- They report any suspected misuse or problem to the Headteacher/Head of School, SLT, Computing Lead or Designated Safeguarding Lead for investigation.
- All digital communications with pupils and parents/carers are on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Acceptable Use policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the set of digital technologies and digital devices in lessons and other school's activities (where allowed) and implement current policies regarding these devices.

3.6 Pupils

Pupils are responsible for:

- Using the school's digital technology systems in accordance with the Pupil Acceptable Use agreement.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

- Knowing and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and cyber bullying.
- Understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
- Elected Digital Leaders support in the leading of technology and computing.

3.7 Parents/Carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet and digital devices in an appropriate way. The school will help parents/carers understand these issues through newsletters, website, and information about both local and national online safety campaigns. Parents/carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video imagery taken at school events.
- Their children's personal devices in the school.

Parent/carers are also expected to:

- Notify a member of staff/headteacher of any concerns of queries regarding this policy
- Ensure their child has read and understood the terms on the Acceptable Use Policy

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites, which are posted on our school website. These have been taken from KCSIE (2025-2026).

Online Safety – Support for Children

- **Childline** – Free and confidential advice for children on any issue, including online safety.
- **UK Safer Internet Centre** – Report and remove harmful online content via the national reporting centre.
- **CEOP Safety Centre** – Report online child sexual abuse directly to the Child Exploitation and Online Protection Command.

Online Safety – Parental Support

- **Childnet Toolkit** – Practical resources to help parents start conversations about online life and find support.
- **Common Sense Media** – Independent reviews, age ratings, and guidance on media, apps, games, and more.
- **Government Advice** – Official guidance on protecting children from online harms including abuse, sexting, and cyberbullying.
- **Internet Matters** – Age-specific safety checklists, parental control guides, and practical tips for digital wellbeing.
- **Marie Collins Foundation – How Can I Help My Child?** – Support for parents of children affected by online sexual abuse.
- **London Grid for Learning** – Online safety tips and presentations for parents, including guidance for primary-aged children.
- **Stop It Now – Lucy Faithfull Foundation** – Resources for parents concerned about sexual behaviour, including early intervention and support.
- **CEOP Education Resources** – Guidance and tools for parents to help protect children from online sexual abuse.
- **ParentZone** – Help and advice for parents navigating the digital world with their children.
- **Children's Commissioner Guide** – A guide to help parents talk to children about online sexual harassment and harmful content.

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Policy Statements

4.1. Educating pupils about online safety

Pupils will be taught about online safety as part of the RHSE, PSHE and Computing curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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

Children can take their responsibilities further by applying to be a Digital Leader. The Computing Lead (Miss Tillson) will liaise with children and teachers to see who would like to apply for the position. Once each class has voted for their Digital Leader, they will take on the role for a year. They will have a responsibility to work with their peers and adults, in addition to their lessons. Their main focus will be internet safety.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.2. Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, via text/Facebook or on Microsoft Teams. This policy will also be shared with parents.

There will be posts for high profile events such as Safer Internet Day, published on Facebook.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Computing Lead and then the Headteacher/Head of School.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Head of School.

4.3. Educating staff about online safety

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal online safety training will be made available to staff. This is regularly updated and reinforced.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.

- The Computing Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- This Online Safety Policy and its updates will be presented to and discussed by staff at relevant meetings.

- The Computing Lead will provide advice, guidance and training to individuals as required.

4.4. Educating governors about online safety

Governors should take part in online safety training and awareness sessions with particular importance for those involved in online safety and safeguarding. This may be offered in several ways:

- Attendance at training provided by the LA/National Governors Association/ or another relevant organisation.

- Participation in school training events.

5. Technical

5.1 Infrastructure/equipment, filtering, and monitoring

The school uses 'Securly' for filtering and monitoring, which covers all devices and identifies any concerns from staff or pupils. This provides full visibility into online activity, download or email reports, and the SLT (Head of School and Assistant Headteachers) receive notifications with flagged content.

Filtering and monitoring reviews should be carried out by the SLT member who is responsible for this (Jade Tillson) along with the DSL and IT support. They should include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record should be kept of these checks. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

The school will be responsible for ensuring the school network is safe and secure as is reasonably possible. They will ensure policies and procedures are implemented. It will also need to ensure the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

- Guests (students, supply teachers, ITT students) may have temporary access on the school systems and will be supported by other teaching staff, e.g., teachers, teaching assistants in class, office staff etc.

- Any content listed as a safeguarding concern is logged and emailed to the Computing Lead, Office Manager and Designated Safeguarding Lead. Any alerts that are a cause for concern are forwarded to the school's Headteacher/Head of School and/or Computing Lead.

5.2 Responsibilities for filtering and monitoring

This guidance has been taken from: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges#:~:text=You%20should%20make%20sure%20that%3A,with%20changes%20to%20safeguarding%20risks

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

The senior leadership team are responsible for:

- scoping the specific needs of their school or college, including use of generative AI
- buying filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- governance of filtering and monitoring systems

- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

A **yearly review** should be conducted by members of the senior leadership team, the designated safeguarding lead and IT support. It should also involve the responsible governor. Checks should be made from both a safeguarding and IT perspective. It will include recording the results of the review and documenting any actions taken. This record should be available to anyone who is entitled to inspect that information. Technical requirements to meet the standard can be found using the link above. The review of filtering and monitoring should be carried out to identify current provision, any gaps, and students' and staff's specific needs. To make this effective, results should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- staff training
- curriculum and learning opportunities
- how often and what is checked
- monitoring strategies
- procurement decisions

As well as taking place once a year, a review should take place when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced, such as new devices or generative-AI tools
- major software updates occur
- there are changes to the technical configuration of the network and devices

A log of the checks should record:

- when the check took place
- who did the check
- what they tested or checked
- resulting actions

SLT should make sure that:

- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before distributing them
- inappropriate content that you choose to block is reviewed and updated in line with changes to guidance and safeguarding risks

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of the setting. There may be a need to ask filtering or monitoring providers for system specific training and support.

The **DSL** should lead on safeguarding and online safety as detailed in the Keeping children safe in education statutory guidance. This should include, among other duties:

- checking relevant reports
- responding to safeguarding concerns identified by filtering and monitoring
- providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

The IT Manager should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT Manager should work with the senior leadership team and DSL to:

- help buy systems
- identify risk
- carry out reviews
- carry out checks

5.3 Mobile Technologies (including BYOD Bring your own phone/BYOT Bring your own technology)

All schools should be **mobile phone-free environments by default**; anything other than this should be by exception only. (KSCIE 2026, 170). Other mobile technologies will be provided by the school, such as the use of iPads and Chromebooks for educational purposes. Teaching about safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

Pupils must not use their mobile phone during the school day. Phones must be handed in as pupils enter school, stored securely in the school office and returned at the end of the day. Misuse will follow the school's behaviour policy.

Staff may bring in personal devices, e.g., their personal mobile phone however it should only be used for personal reasons in designated areas and should be locked away for safeguarding reasons.

The school allows:

	School Devices	Personal devices

	School owned for a single user	School owned for multiple users	Student owned	Staff owned including student teachers	Visitor owned
Allowed in school	Yes	Yes	No*	Yes	Yes
Access to the internet	Yes	Yes	No	No	No

*We appreciate some Year 5/6 pupils may need their mobile phones to communicate with family if they are walking home from school alone. This must be agreed by the Headteacher/Head of School. Items must be labelled, and the school will not be liable for any damage/malfunction of mobile phones.

5.4 Use of digital and video images

This policy applies to all images, including still and video content taken by all staff as well as children and parents/carers.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks.

• When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.

• Permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press. This consent is given when the child starts school and remains with the child unless withdrawn by parents/carers.

All images taken will be used in a manner respectful of the Data Protection Principles. This means that images will be processed:
- Fairly, lawfully and in a transparent manner
- For specified, explicit and legitimate purposes
- In a way that is adequate, relevant limited to what is necessary
- Accurate and up to date
- In a manner that ensures appropriate security

• Parents/carers are welcome to take videos and digital images of **their own children** at school/academy events for their own personal use (as such use in not covered by the Data Protection Act). There are times, however, due to the

circumstances of individual pupils that parents/carers will be asked to refrain from doing so and this will be communicated by school staff.

• Staff and volunteers are allowed to take digital/video images to support educational aims but must follow school's procedures concerning the sharing, distribution, and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.

• Students/pupils must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, Facebook, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Should any inappropriate images be taken, a member of SLT must be notified immediately.

6. Data Protection

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation. See Data Protection Policy.

7. Social Media

7.1 Protecting Professional Identity

Expectations for teachers' professional conduct are set out in 'Teachers Standards'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies and Local Authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools, academies and LAs could be held responsible, indirectly for acts of their employee in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school, academy or LA liable to the injured party. Reasonable steps to prevent harm must be in place.

The Business Manager will provide the following measures:

- Ensuring personal data is not published
  Training is provided including acceptable use, social media risks, checking of settings, data protection, reporting issues
- Clear reporting guidance, including responsibilities, procedures, and sanctions
- Risk assessment including legal risk
- A process created for school social media accounts

Staff should ensure that:

- No reference should be made in personal social media to pupils, parents/carers, or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to schools.
- Security settings on personal social media profiles are regularly checked to minimise the loss of personal data.

7.2 Personal Accounts

Personal communications are those made via a personal email/social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
Personal communications which do not refer to or impact upon schools are outside the scope of this policy.
Where excessive personal use of social media in school is suspected and considered to be interfering with relevant duties, disciplinary action may be taken.

7.3 Monitoring of Public Social Media

As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school.
The school's use of social media for professional purposes will be checked regularly by the Office Team to ensure compliance with the school policies.

7.4 Unsuitable/inappropriate activities

Some internet activity e.g., accessing indecent images of children or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g., cyberbullying 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 age of the users or the nature of those activities.
Our 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 or outside schools when using school equipment or systems. Examples include, but are not limited to, promotion of any kind of discrimination, threatening behaviour, infringing copyright, online shopping, online gambling, creating computer viruses etc.

8. Responding to incidents of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies: the Behaviour Policy and Acceptable Use Policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the [staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Appendices

Appendix 1

School Laptop Declaration

Please read and sign for the loan and use of a school's laptop and equipment. A record of this declaration will be kept in school. Please be aware that laptops will be subject to random checks by senior management and NLLT. Laptops are owned by the school and are to be used by staff to enhance their professional activities including teaching, research, administration and management.

This declaration is to be read in conjunction with the school's "Acceptable Use Policy".
It is required that all school laptops:

- be used primarily for school business and private use shall be ancillary and not significant otherwise tax liabilities may be incurred.
- Should be used for activities appropriate to staff professional needs.
- May be used for personal use at the discretion of the head teacher without damaging the integrity of the school, and school systems.
- Must never be used for accessing or purchasing inappropriate materials such as pornographic, racist or offensive material, or for personal financial gain, gambling, political purposes, advertising, or accessing chat rooms.
- Should only be used by the named person signing this declaration or under strict supervision of this person. The person signing this declaration is solely responsible for any material accessed via the laptop, and to this end, may face disciplinary action should inappropriate use occur.
- Should only be accessible via a password, known only to the user and senior management of the school. I also declare the following:
- I will use the schools e-mail, internet and intranet facilities primarily for business use, and only for personal use during designated break/holiday/home periods in line with ICT use policy.
- I will use only those facilities I am authorised to use.
- I understand that my usage of these facilities may be monitored in accordance with our Data Protection Policy/ICT Use Policy
- I understand this declaration applies to all other mediums and equipment. I am aware and understand the above requirements of the school and local authority, have read guidance, and will adhere to these guidelines.

Name (in print) _____

Signed _____ Date _____

Appendix 2

Chrome Book Sign Out

Name	Chromebook	Date out	Staff Name	Staff Signature	Date in	Staff Name	Staff Signature