September 2025
Review: September 2026

E-Safety and Acceptable Use Policy

1. Development / Monitoring / Review

This policy should be read in conjunction with our Child Protection Policy, our Policy on the Use of Handheld Devices & our Acceptable Use of the Internet Policy. A section within this policy deals with the Acceptable Use of Social Media.

2. Scope of the Policy

This policy applies to all members of the school community (including staff, pupils volunteers, parents & carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers 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 e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the 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 by 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 parents/carers of incidents of inappropriate e-safety behaviour that take place in or out of school.

3. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body, has taken on the role of E-Safety Governor as part of the role as Safeguarding Governor. The role of the E-Safety Governor will include:

- Regular meetings with the Designated Safegaurding Lead (including any e-safety incident logs)

- Reporting to the Full Governing Body.

Head Teacher and Designated Safeguarding Lead (DSL)

- The Head teacher and DSL have a duty of care for ensuring the safety (including e-safety) of members of the school community.

- The Headteacher and DSL should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section).

- The Headteacher and DSL are responsible for ensuring that the E-Safety Coordinator and other relevant staff, receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who may carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The DSL will receive regular monitoring reports from SENSO Cloud and ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- The DSL meets with E-Safety Governor as required to discuss current issues and review incident logs

- The Headteacher and DSL will ensure all staff receive regular updates regarding E-Safety and have responsibility for reviewing and updating E-Safety policies and procedures.

- Attends relevant governor meetings.

E-Safety Coordinator

- The named E-Safety Co-ordinator is: India Hackworth

- Takes day to day responsibility for e-safety issues.

- Provides training and advice for staff under the guidance of the Headteacher and DSL.

- Liaises with the Local Authority.

- Liaises with school technical staff.

Network Manager/ICT Technician

The school network manager is Ben Tait. The Network Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required e-safety technical requirements and any Local Authority E-Safety Policy Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- The use of the network/internet is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher E-Safety Coordinator for investigation.
- Monitoring software systems are implemented and updated as agreed in school policies.

NB: Filtering and monitoring systems are provided by NCC but the network manager must ensure the relevant software is installed on all machines. The Headteacher receives weekly usage reports from NCC.

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy. (see appendix 2).

- They report any suspected misuse or problem to the E Safety Coordinator or Headteacher for investigation.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities.

- Pupils understand and follow the e-safety and acceptable use policies.

- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- 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.

Child Protection Designated Person

The Designated Person for Child Protection is Philip Pallas

The Deputy Designated Person for Child Protection are: Vicky Rowley, Stephanie Bowness and Catherine Johnson

The Designated Person for Child Protection:

- Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:
  - Sharing of personal data.
  - Access to illegal/ inappropriate materials.
  - Inappropriate on-line contact with adults/strangers o potential or actual incidents of grooming.
  - Cyber-bullying.

Pupils

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.

- Are developing a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras.

- Should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

- They should also know and understand policies on the taking/use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to websites that pupils are provided with passwords for.
- Their children's personal devices in the school (where this is allowed).

Community Users

Community Users who access school systems will be expected to acknowledge an Acceptable Use Agreement before being provided with access to school systems.

4. Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing, PHSE and other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information**.**
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- Pupils should be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that 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.
- Where Pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website.
- Parents Evenings
- High profile events/campaigns e.g. Safer Internet Day
- Wake up Wednesday weekly newsletter shared with parents via social media and the school website.
- Reference to the relevant web sites / publications e.g.:-

O www.swgfl.org.uk

o www.saferinternet.org.uk

o http://www.childnet.com/parents-and-carers
o https://www.thinkuknow.co.uk
o https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
https://www.oiam.org/freeschool/latest-news/safeguarding-newsletter

Education – The Wider Community

The school will support opportunities for members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide e-safety information for the wider community.
- Providing workshops/information at events in school.

Education & Training – Staff/Volunteers

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly

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

- The E-Safety Coordinator/DSL receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

- This E-Safety policy and its updates will be presented to, and discussed by, staff in staff meetings and INSET days.

- Under the guidance of the Headteacher/DSL, the E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members involved in e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association, and Governors' E-Learning (GEL).
- Participation in school training/information sessions for staff or parents.

5. Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.

- All users (at KS1 and above) will be provided with a username and secure password by (MB) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 3 months.

- The administrator/master passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (school safe).
- The Headteacher (with Ben Tait) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing

the LA filtering systems. Content lists are regularly updated and internet use is logged and regularly monitored. Only the Headteacher may request changes to this filtering.

- The school has provided enhanced and differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils etc.)

- School technical staff and the DSL regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement using SENSO cloud.

- An appropriate system is in place (all incidents to be reported to E-Safety Co-ordinator/Headteacher currently on paper however once up and running this will be done through CPOMs) for users to report any actual /potential technical incident/security breach.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school network and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Access is only given following an AUP being read and signed. This system allows network access tracking to specific users.

- Personal use of school devices by staff users and their family members out of school is not condoned.

- Staff are also forbidden from downloading executable files and installing programmes on school devices.
- All write function to external media has been disable by the school. This means memory sticks cannot be written to but can be used for resources and planning however the school encourages the use of Office 365 for all file storage as this provides the most secure system.

Use of digital and video images – Please refer to policy on the use of handheld devices

Data Protection - Please refer to separate GDPR policy for more details

Mobile Devices and Communications – Please refer to policy on the use of handheld devices / acceptable use policy

6. Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees 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 or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: 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.

School staff should ensure that:

- No reference should be made in 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 the school or local authority.

- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Safeguarding Governor to ensure compliance with the school policies.

7. 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 technical 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.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the "Reporting an e-Safety Incident Flowchart" provided by Northumberland Local Authority for responding to online safety incidents and report immediately to the police

Other Incidents

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

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures

- Involvement by Local Authority or national /local organisation (as relevant).

- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- Incidents of 'grooming' behaviour

- The sending of obscene materials to a child

- Adult material which potentially breaches the Obscene Publications Act

- Criminally racist material

- Other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

8. Use of Artificial Intelligence (AI)

AI-Related Risks

The school recognises the increasing role of AI in education and online life.
Risks include:

- AI giving confusing, untrue, or unsafe answers.
- Pupils seeing fake or misleading images, videos, or messages.
- AI being used in apps or games in ways that might encourage unkind behaviour or copying other people's work.
- Children being tricked or influenced by AI-generated content.

Safeguards

- The school will follow DfE guidance on **generative AI in education (2025)**.
- All AI usage in school will be subject to the same **filtering and monitoring** requirements as other online tools.
- Staff will be trained to understand the opportunities and risks of AI and will supervise its use in the classroom.
- Pupils in primary school will not use AI tools independently unless directed and supervised by a teacher.
- Any use of AI (e.g. in learning apps or online resources) will be age-appropriate and risk assessed by staff.
- Pupils must never use AI to create or share content without a teacher's permission.
- Personal or sensitive information must never be shared with AI tools.

Pupils will be taught, through Computing and RSHE, to:

- ask a trusted adult if they see something online that is confusing or worrying,
- understand that not everything they see or read online is true (including content made by AI),
- use technology with kindness and respect.

Staff Responsibilities

- Staff must model safe, critical, and responsible use of AI.
- Free, consumer versions of AI platforms (e.g., ChatGPT, Google Gemini, image generators) may not provide sufficient safeguarding, filtering, or data protection. These must not be used with directly with pupils unless formally risk assessed and approved.
- Staff must complete a Data Protection Impact Assessment (DPIA) before introducing any new AI tool into teaching or administrative use.
- Any concerns about inappropriate use of AI (by staff or pupils) must be reported via the school's safeguarding procedures.
- AI should be used to support teaching, learning, and workload reduction, not to replace professional judgment

- See Appendix 7 for further information on the use of AI for staff.

Signed: …… Chair of Governors

On behalf of the Governing Body

Dated: …….

Appendix

1. Acceptable use of the schools ICT systems and internet: agreement for pupils and parents/carers.

2. Acceptable use policy Staff form

3. Acceptable use of the schools ICT systems and internet: agreement for governors, volunteers and visitors

4. E-Safety training needs audit

5. E-safety Incident report log

6. SMART Poster

7. Other E-Safety Posters

Appendix 1

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- I must keep my passwords safe and secure. I will not share it and neither will I try to use someone else's password.
- I will not bring a mobile phone in to school unless I have permission from the head teacher, in which case the mobile phone will be handed in to the school office.
- I agree that the school will monitor the websites I visit.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I will always use the school's ICT systems and internet responsibly
- I will follow the school's Zip it! Block it! Flag it! System to help me stay safe online and report any incidents to my class teacher.

Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved.

- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher.
- It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- School devices should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc, CD Rom or external memory device should be brought in from home for use in school.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 2

Stead Lane Primary School

Acceptable Use Policy

Staff Form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet /network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business.
- I will only use the approved email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the e-safety co-ordinator.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended antivirus, firewall and other ICT 'defence' systems.
- I will ensure that any school laptop/other equipment loaned to me is password protected and not accessible by others when in use at home and that it is not used inappropriately by myself or others.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / NCC advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data which I need to access is held securely in Google drive and will not be transported by an external device such as USB stick, in line with school protocols.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.

- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

……User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

The use of digital / video images plays an important part in school activities. Digital devices may be used to record activities in lessons and out of school. These images may then be used in presentations or used to celebrate the successes of the school through their publication, for example, in newsletters, school prospectus, on the school website, online learning journals in Early Years and occasionally in the public media.

- I agree to the school taking and using digital / video images of me. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school, for example in the school prospectus, website and media

Signature: ..... Date: .....

Full Name (printed): .....

Job title: .....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature: ….. ……..... Date: ……

Full Name (printed): …….. .....

Appendix 3

Acceptable use of the school's ICT systems and the internet: agreement for governors, volunteers and visitors

Name of governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details
- I will only use the school's ICT systems and access the internet in school, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit.
- I will not use any external devices such as USB devices.
- I will let the e-safety co-ordinator know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

……

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account (governor only); be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

The use of digital/video images plays an important part in school activities. Digital devices may be used to record activities in lessons and out of school. These images may then be used in presentations or used to celebrate the successes of the school through their publication, for example, in newsletters, school prospectus, on the school website, online learning journals in Early Years and occasionally in the public media.

- I agree to the school taking and using digital/video images of me. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school, for example in the school prospectus, website and media

Signed (governor/volunteer/visitor):	**Date:**

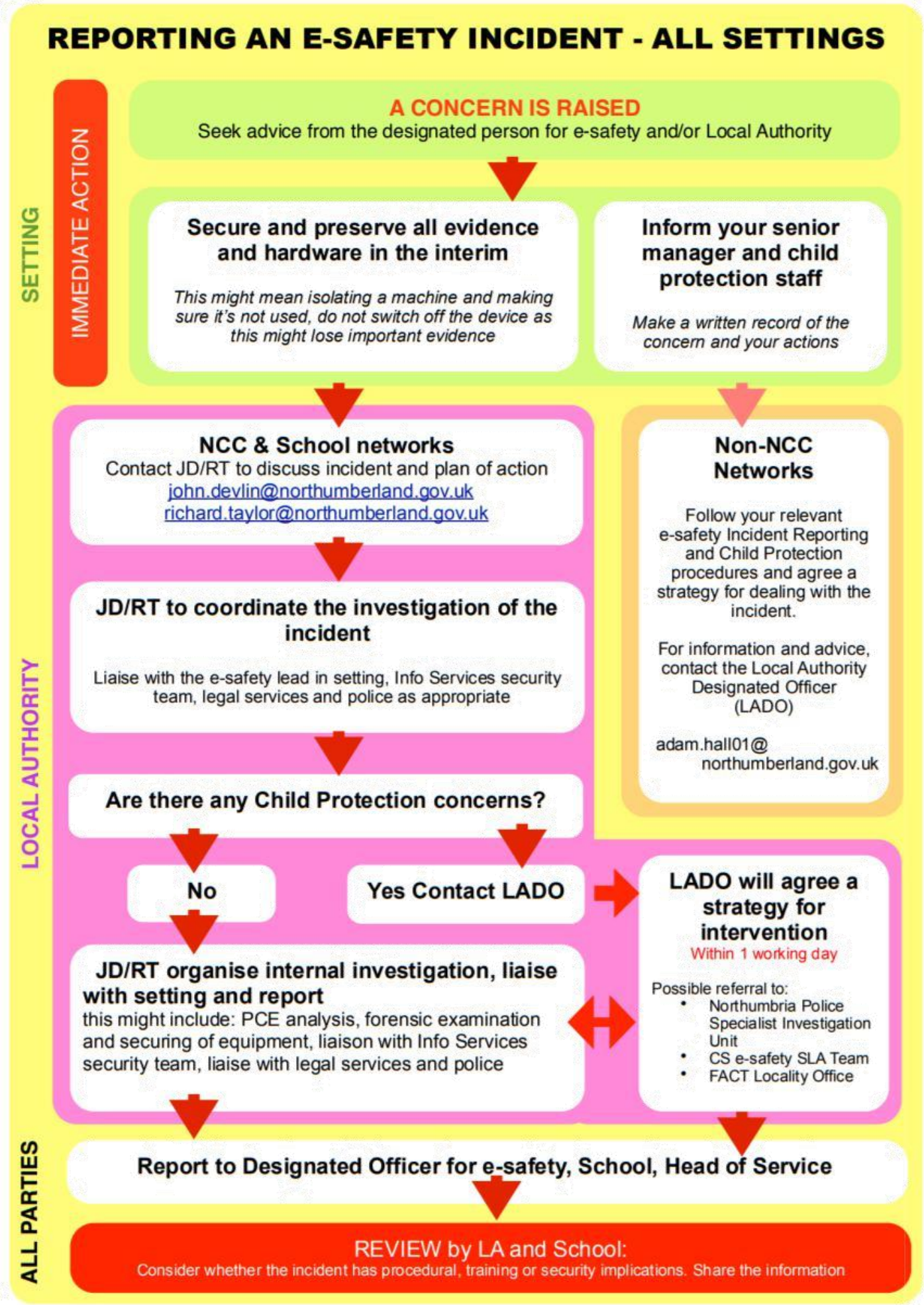
Signed (Head Teacher)	**Date:**

Appendix 4

E-safety training needs audit	
Name of staff member/Governor/Volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5

E-safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staf member recordin the incident


REPORTING AN E-SAFETY INCIDENT - ALL SETTINGS
SETTING
IMMEDIATE ACTION
A CONCERN IS RAISED
Seek advice from the designated person for e-safety and/or Local Authority
Secure and preserve all evidence and hardware in the interim
This might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence
Inform your senior manager and child protection staff
Make a written record of the concern and your actions
LOCAL AUTHORITY
NCC & School networks
Contact JD/RT to discuss incident and plan of action
john.devlin@northumberland.gov.uk
richard.taylor@northumberland.gov.uk
Non-NCC Networks
Follow your relevant e-safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.
For information and advice, contact the Local Authority Designated Officer (LADO)
adam.hall01@northumberland.gov.uk
JD/RT to coordinate the investigation of the incident
Liaise with the e-safety lead in setting, Info Services security team, legal services and police as appropriate
Are there any Child Protection concerns?
No
Yes Contact LADO
LADO will agree a strategy for intervention
Within 1 working day
Possible referral to:
Northumbria Police Specialist Investigation Unit
CS e-safety SLA Team
FACT Locality Office
JD/RT organise internal investigation, liaise with setting and report
this might include: PCE analysis, forensic examination and securing of equipment, liaison with Info Services security team, liaise with legal services and police
ALL PARTIES
Report to Designated Officer for e-safety, School, Head of Service
REVIEW by LA and School:
Consider whether the incident has procedural, training or security implications. Share the information

Be smart on the internet

Childnet International
www.childnet.com

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows.

T TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

www.kidsmart.org.uk

KidSMART

Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.


Be
SAFE
Online
1 I only go online with a grown up
2 I am kind online
3 I keep information about me safe
4 I tell a grown up if something online makes me unhappy
eis Kent
Education IT Services
Kent County Council
kent.gov.uk
Published by EIS Kent • 0300 065 8800 • www.eiskent.co.uk