Amble Links First School
Policy for E-Safety

Date Written: **March 2017**
By: **Paul Heeley**
Responsible Governor: **Safeguarding (Barrie Cooper)**
Adopted by Governors: **March 13 2017**
Date for Review: **March 2018**

Development / Monitoring / Review of this Policy
This e-safety policy has been developed by a working group including:

- Headteacher / E-Safety Co-ordinator
- Staff – including Teachers, Support Staff and Technical staff
- Governors

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development /Monitoring /Review

This e-safety policy was approved by the Governing Body	March 2017
The implementation of this e-safety policy will be monitored by:	Paul Heeley (Headteacher/Designated Safeguarding Lead) Louise Lightley (Deputy Designated Safeguarding Lead) Barrie Cooper (Governor - Safeguarding) John Harwood (Technician)
Monitoring will take place at regular intervals:	Weekly log monitoring.
The Safeguarding Governor will receive a report on the implementation of the e-safety policy on a termly basis. The content of this report will be included in the termly Safeguarding report to the Full Governing Body.	Termly
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	March 2018
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	John Devlin (LA E-Safety Consultant). Police Local Authority Designated Officer (LADO) preventmailbox@northumbria.pnn.police.uk

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity –Reports from Policy Central Enterprise Software
  - Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

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.

This policies ensures that the school meets and exceeds the requirements for online safety set out in Annex C of 'Keeping Children Safe in Education (Sept 2016)'.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. **This is pertinent to incidents of cyber-bullying or other 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 school's 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.

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 (Barrie Cooper) 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 E-Safety Co-ordinator/Designated Safeguarding Lead
- regular monitoring of e-safety incident log.
- regular monitoring of filtering change control logs.
- reporting to the Full Governing Body.

Headteacher
- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team (Louise Lightley) 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).
  SWGfL BOOST (a software package purchased by the school) includes an 'Incident Response Tool' that steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow.
- The Headteacher is 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.
  SWGfL BOOST includes access to unlimited online webinar training.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who 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. This will include training on the use of the Policy Central Enterprise (PCE) monitoring tool.
- The Headteacher will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher will ensure that filtering, tracking and monitoring systems are in place to support delivery of the PREVENT agenda to prevent pupils and staff being drawn into radicalisation and extremism.

E-Safety Coordinator
The named E-Safety Co-ordinator is: **Paul Heeley**
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school technical staff.

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments. SWGfL BOOST includes access to Whisper, an anonymous reporting app that installs onto a school website and extends the schools ability to capture reports from staff, children and parents.
- ensures that filtering, tracking and monitoring of ongoing logs supports delivery of the PREVENT agenda to prevent pupils and staff being drawn into radicalisation and extremism.
- meets regularly with E-Safety/Safeguarding *Governor* to discuss current issues, review incident logs and filtering.
- attends relevant governors meetings.
- reports regularly to the Headteacher.

Network Manager/ICT Technician)
The school network manager is **John Harwood** (Harwood Technical Services)

The Network Manager is responsible for ensuring:
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority E-Safety Policy Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- that 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.
- that 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.
- that monitoring software systems are implemented and updated as agreed in school policies.

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.
- they report any suspected misuse or problem to the 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.
- all staff are expected to adhere to the 'E-Safety – Social Media Guidance' produced by the Northumberland Safeguarding Children Board (NSCB). Available on the staffroom noticeboard.

Child Protection Designated Person
The Designated Person for Child Protection is **Paul Heeley**.

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
    - potential or actual incidents of grooming
    - cyber-bullying.
    - child sexual exploitation
    - radicalisation and extremism

Pupils:

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

Community Users

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

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 programme of assemblies.
- Pupils should be taught strategies to recognise and report any situations which may be aimed at drawing them towards radicalisation and extremism as part of the PREVENT agenda.
- 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 (eg 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
- An area of the school website dedicated to E-Safety
- Letters, newsletters, School360
- Parents Evenings
- High profile events/campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers.

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:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety.
- 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.

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.
  SWGfL BOOST includes unlimited online webinar training for all, or nominated staff. Some staff may identify e-safety as a training need within the performance management process.
- 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.
  SWGfL BOOST includes an array of presentations and resources that can be presented to new staff.
- The E-Safety Coordinator receive 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.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.
  SWGfL BOOST includes an array of presentation resources that the e-Safety coordinator can access to deliver to staff.

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.

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 academy technical systems and devices.

- All users (at KS1 and above) will be provided with a username and secure password by John Harwood (Technician) 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 90 days.
- The administrator 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 John Harwood) 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 Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored through Futures Cloud software. 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 E-Safety Co-ordinator 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 Futures Cloud.
- An appropriate system is in place (all incidents to be reported to E-Safety Co-ordinator/Headteacher) for users to report any actual /potential technical incident/security breach to the relevant person, as agreed).
- 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" (eg 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 allowed.
- Staff are also forbidden from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (eg memory sticks /CDs/DVDs) by users on school devices. Any removable media used must be encrypted. Staff are strongly encouraged to only use secure cloud based storage through School360/Google. Personal data cannot be sent over private email addresses or taken off the school site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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 eg on social networking sites**.**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students/pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes. The only exception to this is the use of the Headteacher's mobile phone to take images that can immediately be uploaded to the school website and Facebook page – permission for this has been granted by all parents.
- Care should be taken when taking digital /video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing.
- It has a Data Protection Policy.
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs).
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected.
- the device must be password protected.
- the device must offer approved virus and malware checking software.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Mobile Devices and Communications

We have a separate policy for the use of mobile devices in school.

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
  SWGfL BOOST includes an anonymous reporting app 'Whisper'.
- Any digital communication between staff and pupils or parents/carers (email,chat,VLE etc) must be professional in tone and content.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use –these email addresses are restricted to only communicating with other users within a secure environment (School360).
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

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. SWGfL BOOST includes unlimited webinar training on this subject.
- 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 /academy 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 Social Media, Data Protection, Communications, Digital Image and Video Policies. SWGfL BOOST includes SWGfL Alerts that highlight any reference to the school in any online media (newspaper or social media) for example.

Unsuitable/inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section may be inappropriate in a school context and that users, or groups of users, as defined below, may not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and Illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts					X

against children Contrary to the Sexual Offences Act 2003.					
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
Promoting radicalisation or extremism				X	X
Pornography				X	
Promotion of any kind of discrimination				X	
Threatening behaviour, including promotion of physical violence or mental harm				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing				X	
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

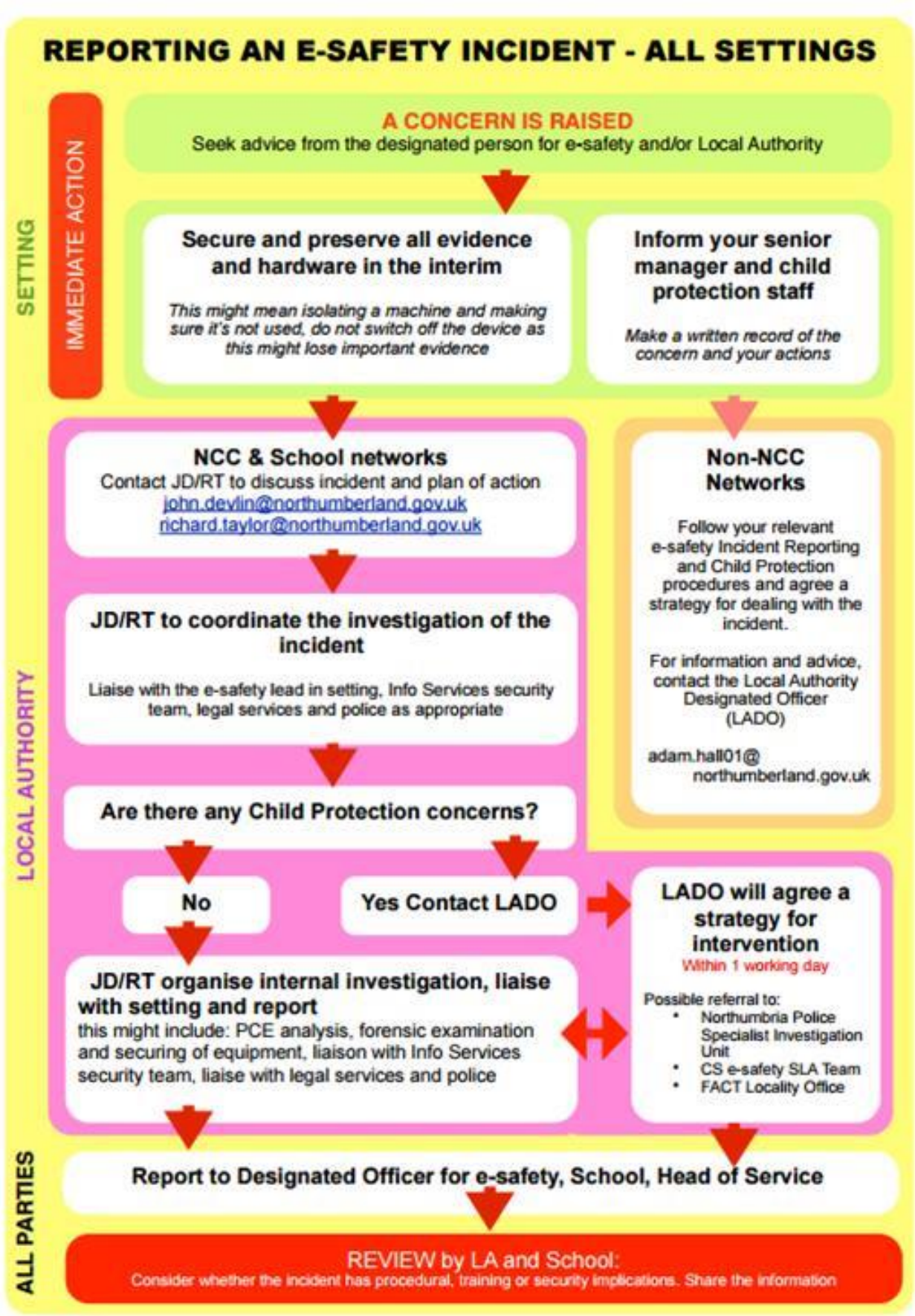
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents.

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 Flowchart (below) 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.

Where there are concerns that the promotion of radicalisation or extremism is taking place this should be reported immediately in line with the school's policies for Child Protection and 'Tackling Extremism and Radicalisation' policy that support the **PREVENT** agenda. Concerns should immediately reported to the Local Authority Designated Officer (LADO) – Adam Hall (01670 62397) or to the police: preventmailbox@northumbria.pnn.police.uk.

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. The table below identifies likely procedures that would be followed in such cases.

Staff

Incidents:	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to technical support staff for action re filtering / security etc	Warning	Suspension	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).	X	X	X	X		X	X
Inappropriate personal use of the internet/social media/ personal email	X			X			
Unauthorised downloading or uploading of files	X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X			X	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X				X		X
Deliberate actions to breach data protection or network security rules	X	X			X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X		X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X
Involvement in the promotion of radicalisation or extremism	X	X	X	X	X	X	X
Using personal email/social networking /instant messaging/ text messaging to carrying out digital communications with pupils	X	X	X		X	X	X
Actions which could compromise the staff member's professional standing	X				X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X
Using proxy sites or other means to subvert the school's filtering system	X	X		X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	X
Breaching copyright or licensing regulations	X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X	X

Pupils

Incidents:	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /inappropriate activities).		X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X							
Unauthorised use of mobile phone / digital camera / other mobile device		X						
Unauthorised use of social media / messaging apps / personal email	X							
Unauthorised downloading or uploading of files		X						
Allowing others to access school / academy network by sharing username and passwords		X		X		X		
Attempting to access or accessing the school / academy network, using another student's / pupil's account		X				X		
Attempting to access or accessing the school / academy network, using the account of a member of staff		X			X	X		
Corrupting or destroying the data of other users		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X			X	X	X	X
Involvement in the promotion of radicalisation or extremism		X	X	X	X	X	X	X

Acknowledgements

This policy is based on model policies provided by SWGfL.

This policy should be reviewed annually.

A COPY OF THIS POLICY IS AVAILABLE IN LARGE PRINT ON REQUEST