Scremerston First School

E-Safety Policy

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Governing Body: February 2016.
Monitoring of the E-Safety Policy will take place at regular intervals.
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 school will monitor the impact of the policy using:
•Logs of reported incidents.
•Monitoring logs of internet activity (including sites visited) via PCE provided by NCC.
•Surveys/questionnaires of:
•students
•parents/carers
•staff
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

Scope of the Policy

This policy applies to all members of Scremerston First School (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Scremerston First Schools' ICT systems, both in and out of the School. The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Discipline and Bullying, Curriculum, Data Protection and Security.

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 (George Dance) 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..
- 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 (Emma Holleywell- who is also DSL support) 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 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.
- 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: **Emma Holleywell**

- 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.
- that the use of the internet is regularly monitored in order that any misuse/attempted misuse can be reported/ recorded appropriately for investigation.
- provides training and advice for staff.
- liaises with the Local Authority.
- liaises with school technical staff (David Harrison technician)
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

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 *Governor* to discuss current issues, review incident logs and filtering.
- attends relevant governors meetings.
- reports regularly to the Headteacher.

ICT Technician
The school ICT technician is **David Harrison.**
The ICT technician 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 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 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 or e-safety coordinator 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 **Helen Harrison**, in her absence it is **Emma Holleywell.**
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.

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 be taught about appropriate conduct when taking/using of images and be aware of what cyber-bullying is, its implications and how to report this.
• 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/ school 360 that pupils are provided with passwords for.

The use of personal devices by children in school is prohibited unless otherwise arranged with Helen Harrison- Headteacher.

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. All children to have access to specific e-safety lessons at least once per term.

• 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:

- The school website will contain information on e-safety.
- The school will advertise local e-safety events/ training.

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:

• An audit of the e-safety training needs of all staff will be carried out regularly. From this e-safety staff/ teacher meetings will be planned accordingly.

• 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 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.

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 equipment, internet and infastructure 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.
- The Headteacher/ Julia Bradbury (School Admin) 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.**
- The Headteacher and E-Safety Co-ordinator regularly monitor the activity of users on the school technical systems via the PCE reports and users are made aware of this in the Acceptable Use Agreement using Policy Central Enterprise.
- An appropriate system is in place (all incidents to be reported to E-Safety Coordinator/Headteacher) for users to report any actual /potential technical incident/security breach to the relevant person, as agreed). A log book is kept in the staffroom for staff to record any technical issues. This is reviewed fortnightly by David Harrison. An e-safety incident log is located in the e-safety file. EH and HH to keep dated records of any e-safety incidents.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are updated and tested regularly.
- 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. Guests will be given a temporary password to access devices.
- 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. 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.
- 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:

• Any digital communication between staff and pupils or parents/carers (email,chat,VLE etc) must be professional in tone and content.

Mobile devices and communications conduct is outlined in the schools AUP.

• 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.

• Pupils at KS2 and above will be provided with individual school email addresses, via School360, for educational use.

• 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.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Included in audit of staff training.

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.

Appropriate and Inappropriate Use by Staff or Adults:
Staff members have access to the network so that they can obtain age appropriate resources for their classes and create folders for saving and managing resources. They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement,
which they need to sign, return to the school, AUPs may be accessed at any time from the office via Julia Bradbury.
When accessing the Learning Platform "School 360" from home, the same Acceptable Use Agreement will apply.

In the Event of Inappropriate Use
If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher/e-safety coordinator immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Appropriate and Inappropriate Use by Children:
Acceptable Use Agreements detail how children are expected to use the internet and other technologies within school, including downloading or printing of any materials. The agreements are there for the children to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.
School should encourage parents/carers to support the agreement with their child or young person. We will do this by providing an AUP form for the children and their parent/ carer to sign together so that it is clear to the school/education setting or other establishment that the agreements are accepted by the child with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children may be using the Internet beyond school/education setting or other establishment. Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.
The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

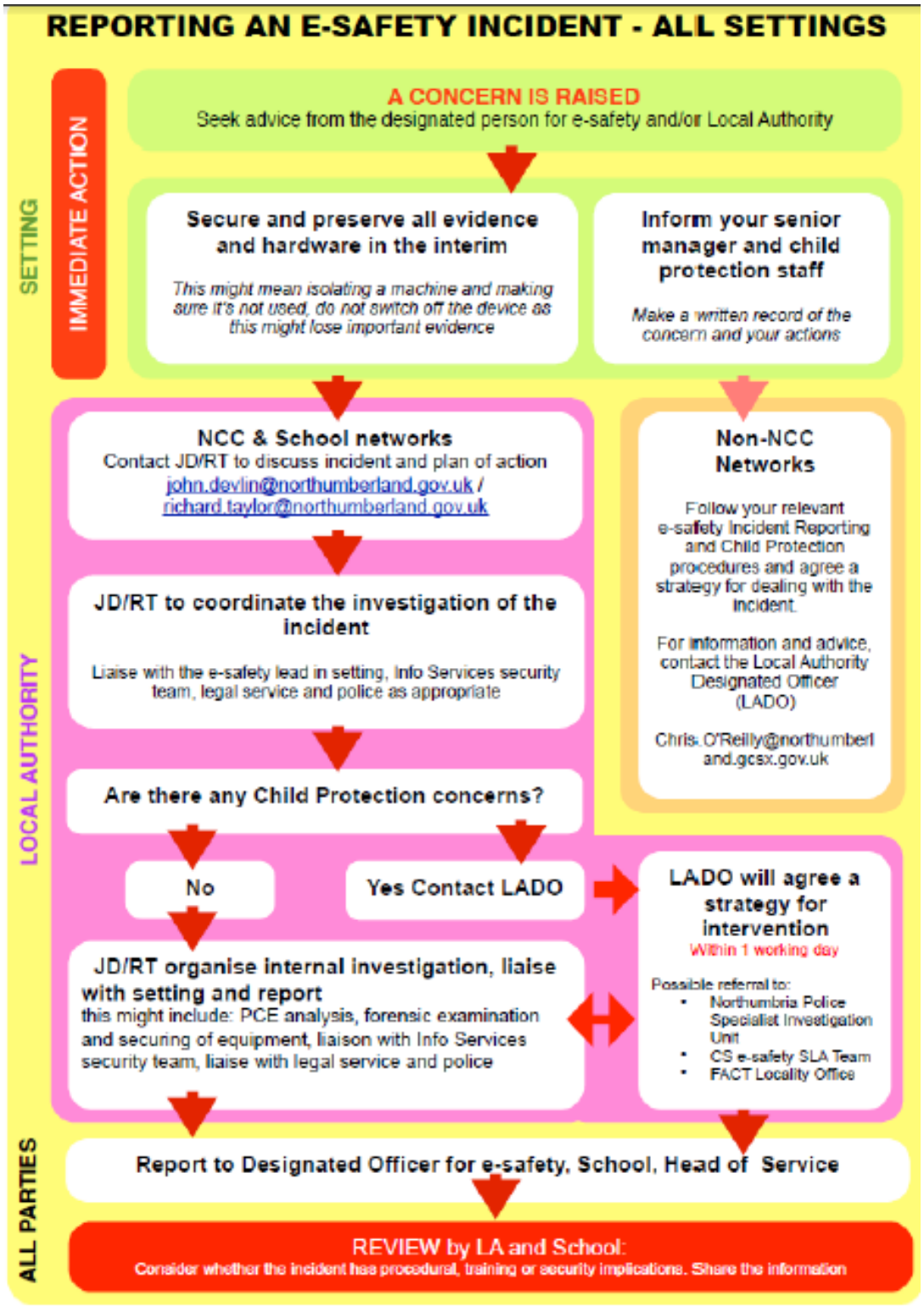
In the Event of Inappropriate Use

In the event of a child to be found using the school internet facilities inappropriately, either Helen Harrison or Emma Holleywell must be informed. Each case will be looked at individually in discussions with EH and HH. Appropriate sanctions will be put in place and the policies and procedures reviewed.

If a child is found to repeatedly abuse the school internet facilities, this may result in loss of internet access/ privileges and a parent/ carer will need to be contacted.

In the event that a child or young person accidentally accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

All e-safety incidents must follow the e-safety incident flow chart as attached. This flow chart is also displayed in the staffroom.



Acknowledgements
This policy is based on model policies provided by SWGfL.

Co-ordinator: Helen Harrison

Date: March 2007	**Review Date: March 2008**
Reviewed: September 2009	**Review Date: September 2010**
Reviewed: September 2010	**Review Date: September 2011**
Reviewed: September 2011	**Review Date: September 2012**
Reviewed: September 2012	**Review Date: September 2013**
Reviewed: September 2013	**Review Date: September 2014**
Reviewed: September 2014	**Review Date: September 2016**
Reviewed: September 2015	**Review Date: September 2017**
Reviewed: February 2016	**Review Date: February 2018**
Reviewed: September 2017	**Review Date: September 2019**