E-SAFETY POLICY

The governing body of the Ashington Learning Partnership fully recognises its responsibility for e-safety issues.

Scope of the Policy
This policy applies to all members of the trusts community including staff, pupils, volunteers, parents, carers and visitors who have access to, and are users of ICT systems and equipment both on and off the grounds of Bothal Primary School or Central Primary School.

Rationale
E-safety encompasses the use of new technologies, internet and electronic communications such as mobile phones and tablet devices, collaboration tools, social networking and personal publishing. It highlights the need to educate staff, pupils and Governors about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

As pupils' confidence in the use of technology increases, it becomes more important that we control its use within school and educate pupils and staff about using it safely outside that environment. As such, we seek to provide systems which can educate pupils in this manner whilst providing a monitored, controlled and secure environment such as the VLE.

This e-safety Policy will operate in conjunction with, and offer intended overlap with, other policies including those for Behaviour, Anti-Bullying, Data Protection, Safeguarding and the staff, pupil and visitor Acceptable Use Policies.

- The Internet and use of new technology are essential elements in 21st century life for education, business and social interaction. The Trust has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils. The use of computers, tablets and mobile phones can also enhance the education of our pupils and should be encouraged as long as suitable controls are in place.
- Pupils and staff use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Roles and Responsibilities
The Executive Principal will be the person with the overall responsibility for the safety of the school community. This will then be delegated, as appropriate, to other specific members of staff including the e-safety Co-coordinator and the e-safety Group.

E-safety Co-ordinator/Group
- Ensure leadership team is aware of the procedures that need to be followed in the event of an e-safety incident occurring.
- Provide a "first port of call" service for any e-safety concerns or incidents.
- Keep up to date with changes to e-safety and any relevant technologies with a view to presenting them at e- Safety Group meetings.
- Provide training for staff and parents in accordance with the e-safety Policy and Standard Operating Procedures.

- Provide e-safety curriculum content throughout the year for all key stages.
- Support the curriculum and teachers in delivering e-safety content throughout the year.
- Provide cross-curricular e-safety content for other subjects.
- Ensure that staff, visitors and pupils have signed Acceptable Use Policies.

Designated Child Protection Officer (Member of the e-safety Group)

- Take responsibility for dealing with e-safety incidents which lead to child protection issues. Seek support from e-safety Coordinator, leadership teams and the local authority where necessary.
- Keep up to date with this e-safety Policy and have a working knowledge and understanding of the other associated policies.
- Contribute to the review of e-safety polices in light of any changes to safeguarding policies or procedures.

E-safety Governor

- Annual meeting to scrutinise e-safety provision.
- Complete regular online training for e-safety.

Education and Training

An e-safety training programme is in place for all members of the school community.

Pupils

Pupils will be taught online safety as part of the computing curriculum and should be regularly revisited. Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- e-safety rules and relevant, up to date signage will be posted in all computer suites and highlighted to the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored and where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Staff

- Child protection training completed annually, or more often in the advent of changes to procedure, will include an element of e-safety and Prevent training.
- Staff will be trained to understand their role and responsibilities with regards to e-safety; who they should speak to if they are made aware of an e-safety incident and how they can support pupils with such concerns.

Parents

- Parents' attention will be drawn to the e-safety Policy in newsletters, prospectuses, and on the school website.
- Appropriate training will be offered to parents and information updates sent home on a regular basis.

Governors

- Governors will be provided with online e-safety training.

Technical Infrastructure

Safety and security of IT systems:

- ICT systems' capacity and security will be reviewed regularly.
- Virus protection and operating system updates will be applied regularly, automatically. Such automated systems will be reviewed regularly.
- All pupils at KS1 and above will be provided with a username and secure password, this will be in the form of a set username and password managed by the IT Co-coordinator or Infrastructure Manager
- The domain administrator passwords for each school will be written down, put into an envelope and secured in a safe
- The Infrastructure Manager is responsible for ensuring that software and hardware audit inventories are up to date and accurate.

Filtration and monitoring

- The Infrastructure Manager will work with Northumberland County Council, the DCSF and the Internet Service Provider to ensure systems to protect pupils are regularly reviewed and improved.
- Changes to filtration requests must be requested via the Infrastructure Manager
- If any community member (staff, pupils, etc.) discovers an unsuitable site, it must be reported to the Infrastructure Manager, e-safety Coordinator or the Designated Child Protection Officer.
- Any community member with a login to the VLE may use the "E-safety Centre" "Whisper" or "Tootoot" links to log anonymous concerns.
- The E-safety Coordinator and Infrastructure manager will regularly check to ensure that the filtering methods selected are appropriate, effective and reasonable, to ensure high quality education while keeping pupils safe.
- All computer use within the schools and on school-owned devices will be monitored using Policy Central Enterprise.
- A weekly summary report will be reviewed by the Designated Child Protection Officer and ICT Coordinator.
- Internet usage will be monitored on a regular basis as per the acceptable use policy

Management of ALP VLE, Google systems and other learning environments

For this section, Systems refers to the school's Virtual Learning Environment

- Usage of the Systems by pupils and staff will be regularly monitored in all areas, in particular message and communication tools and publishing facilities.
- All users will be advised on acceptable conduct when using the Systems.
- Only members of the current pupil, staff and governor community will have access to the Systems.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Systems.
- When community members (staff, pupils, etc.) leave the school their account or rights to specific school areas will be disabled and deleted
- Where Apps are used, all data including images will be kept securely on servers hosted by the app and subject to their own policies for example Tapestry, Earwig, Seesaw

Personal Devices

- Staff may have work email, calendars and documents on mobile devices or tablets subject to level of password protection. Under these circumstances, staff should not share their password with anyone else, nor let them use the device. They should be aware that if they lose the device while it is unlocked then their information is unprotected; suitable care should be taken.
- Staff may not use their own personal devices to taken any photos or videos of pupils. Refer to the Personal Device Policy for more information.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, GDPR and the Data Protection Policy.
- Pupil and staff personal data will not be displayed, physically or electronically, in public areas or areas where visitors or pupils have access.
- Access to the schools' MIS systems will be password protected. Staff should always lock computers when they leave them unattended.

Published Content

- The contact details on school websites should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The designated person will take overall editorial responsibility for the school's website and ensure that content is accurate and appropriate.
- When celebrating pupils' achievements in school, pupils' first names may be published in the school newsletter as long as there is no accompanying photograph. See Use of Images policy

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the school website in association with photographs. This is permitted on the VLE which is only accessed by approved users within the school community and is monitored.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or checked against each schools use of pupil image form or parent/carers acceptable use agreement. See Use of Images Policy
- Staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images

Communication

- Staff should only use their school e-mail accounts for business purposes. E-mail sent to parents or an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chain letters or spam is not permitted.
- Personal mobile phones should not be used to contact parents or pupils. If this is unavoidable then the school's Designated Child Protection Officer or ICT Coordinator should be informed promptly. Under no circumstances should pupil phone numbers be stored on personal mobile phones.
- Mobile phones will not be used during lessons or formal school time
- Normal school sanctions apply to the use of technology (e.g. the sending of abusive or inappropriate text messages).

Social Media

- Access to social networking and forums on any school VLE systems will be controlled by the ALP IT Team and will be used for educational purposes or for named staff to post on the school's behalf, see Social Media Policy for named users and See Social Networking Policy for advise to staff outside of work.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be given guidance on the use of social network sites outside school and this should be age-appropriate.
- Staff should never communicate with pupils through social networking sites outside school. If this is necessary (for example due to involvement in external clubs) then the school's Designated Child Protection Officer should be informed. VLE systems should be used for staff-pupil communication and its use encouraged.
- No reference should be made in social media to pupils, parents / carers or other ALP staff, nor to the school itself.

- Staff should not engage in online discussion regarding personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Staff should be thoughtful and responsible in their personal use of social networking (see Code of Conduct) and ensure that they do not compromise themselves or the school. In particular, care should be taken in interaction with parents, ex-pupils and other members of the local community. Staff must not mention pupils or disclose any confidential information about the school. Any 'friend requests' from pupils should be declined and blocked. Any concerns should be raised with the E-safety Coordinator or Designated Child Protection Officer.
- Staff should ensure that they take appropriate security measures when using external social networking sites so that they protect themselves. https://staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks
- Staff should inform and educate students about the risks attached in publishing their own images on the internet in places such as social networking sites.

Emerging Technologies

- Emerging technologies will be examined for educational benefit and the risks and benefits will be considered before use in school is allowed.

Responding to Incidents of Misuse

Handling e-safety incidents

- Incidents and complaints of Internet misuse will be dealt with by the Designated Child Protection Officer or other member of Senior Leadership Team in conjunction with e-safety Coordinator
- Any incident or complaint about staff misuse must be referred to the Executive Principal and may be referred to the LADO.
- Incidents and complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- The school will adopt the NCC procedures for dealing with e-safety issues (see incident management flowchart appendix 1)

Cyber-bullying

- Cyber-bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the schools' policy on anti-bullying.
- There will be clear procedures in place to support anyone affected by Cyberbullying.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. The Police will be contacted if a criminal offence is suspected.
- All incidents of cyber-bullying reported to the school will be dealt with in accordance with the Behaviour Policy.

Chair of GB Signed | | Date | |

Date:	03 Oct 16	20 Jul 17	
Version	1	2	
Author:	e-safety Group	e-safety Group	
Status:	Draft	Draft	

Appendix 1

Incident Management Flow Chart