Let your light shine' – Matthew 5:16

Whitley Memorial CE Primary School
E-Safety Policy

Our Vision

As a Church of England school our historical roots are vital to our identity and we are committed in serving our community. As a Church of England School, we value all of God's children, and follow our vision of equality for all. We believe that at Whitley Memorial Church of England Primary we are one big family, the 'Whitley Family,' striving to support our children equally in their spiritual and personal growth alongside their academic development.

Our school motto of 'Let your light shine' comes from Matthew 5:16: 'Let your light so shine before all people, that they may see your good works, and glorify your Father which is in heaven.'

This voices our overarching belief that everyone, no matter what their starting point may be, has God given skills and talents and we passionately believe in working collaboratively with parents, learners, members of the community, our church (St Cuthbert's), educational partners and other professionals to ensure all children receive the very best start to their learning journey and have every opportunity to 'Let Your Light Shine.'

Core Values

Our core values are at the heart of our school ethos and Christian environment. These values form the scaffold of our half-termly Worship themes and are also taught explicitly throughout the school. Our values are: *Thankfulness, Trust, Perseverance, Justice, Service, Truthfulness, Generosity, Compassion, Courage, Forgiveness, Friendship and Respect.*

Statement of intent

Whitley Memorial C of E Primary School believes that all children need the tools to be able to cope in an increasingly 'online' world. As a Church of England school we aim equip children not only with vital knowledge but also the moral and spiritual understanding that will enable them to do what is right.

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our e-Safety Policy, as part of the wider safeguarding agenda, outlines how Whitley Memorial Primary School will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

What is e-Safety?

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

The school's e-safety policy will operate in conjunction with other policies including those for Computing, Behaviour, Bullying, Curriculum, Data Protection and Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband connections including filtering.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils across the school.
- The filters are very strict and controlled by the LA.
- Staff and pupils have different access rights to the Internet in school, for example pupil logins are automatically blocked for sites such as You Tube but staff logins have access.
- 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
- Pupils will be taught how to evaluate Internet content
- 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.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly by Northumberland NCC
- Security strategies will be discussed with the Northumberland IT Team

E-mail

- Pupils only learn about e-mail through using internal software within the school network.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff will use authority e-mails in all official communications this is currently name@whitley.northumberland.sch.uk
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site and Facebook page

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils' personal information will not be published.
- The Head Teacher and Computing Lead will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not include pupils whose parents have not given permission
- Pupils' names will not be used anywhere on the website or Facebook page, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/Facebook page.

Social networking and personal publishing

- The school will block access to social networking sites for pupils.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised and explicitly taught never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

- SENSO is used across the county network and NCC uses a strict filtering system.
- Any violations are reported weekly to the Head Teacher and Computing Lead.
- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the eSafety Lead.
- Any breaches of e-safety will follow the NCC Incident Reporting guidelines
- The e-Safety Lead and computer technician, in conjunction with the Northumberland IT Team will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff phones may be used on a school visit in an emergency but the 'Acceptable Use Policy' must be adhered to.

- Staff are not permitted to use their own mobile phones at any time during school hours (see Acceptable Use Policy) except when accompanying children on a school trip.

Protecting personal data and GDPR

- Personal data will be recorded, processed, transferred and made available according to GDPR regulations 2018.
- Where ever possible personal data will be stored only on encrypted storage devices and on password protected hardware.
- On-line back up to 'cloud storage' must comply with current GDPR regulations.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school IT resource, including PCs, iPads, iPods and laptops.
- At Whitley Memorial Primary School any access to the Internet will be closely supervised by teaching staff.
- Children have directly supervised access to specific, approved on-line sites and materials eg NorTLE, School360.
- Visitors to the school have no access to the computer system or Internet unless we provide them with login details.
- Supply staff have a specific login which does not access any of the school's confidential shared folders and drives.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- In the event of an e-safety issue all staff will refer to Responding to e-Safety Incident/ Escalation Procedures (Appendix 1)
- E-safety incidents will be recorded in the e-Safety Incident Log (Appendix 2)

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents will be informed of the complaints procedure (available on Website)

Communications Policy

Introducing the e-safety policy to pupils

- E-safety will be taught across all year groups (Reception – Year 6) at the beginning of each year.
- E-safety rules will be posted in classrooms and on displays and discussed with the pupils at the start of each year.
- Pupils will be given age appropriate information, linked to their e-safety teaching, to take home and share with parents.
- All pupils (Year 1- Year 6) must log on to the computers and network using their own login name and password.
- Pupils will be informed that Internet use will be monitored.
- Year 5 & 6 pupils will be expected to sign the pupil AUP.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All teaching staff will be expected to sign the school's AUP.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.
- Information about e-safety will be sent home to parents and be made available on the school website.

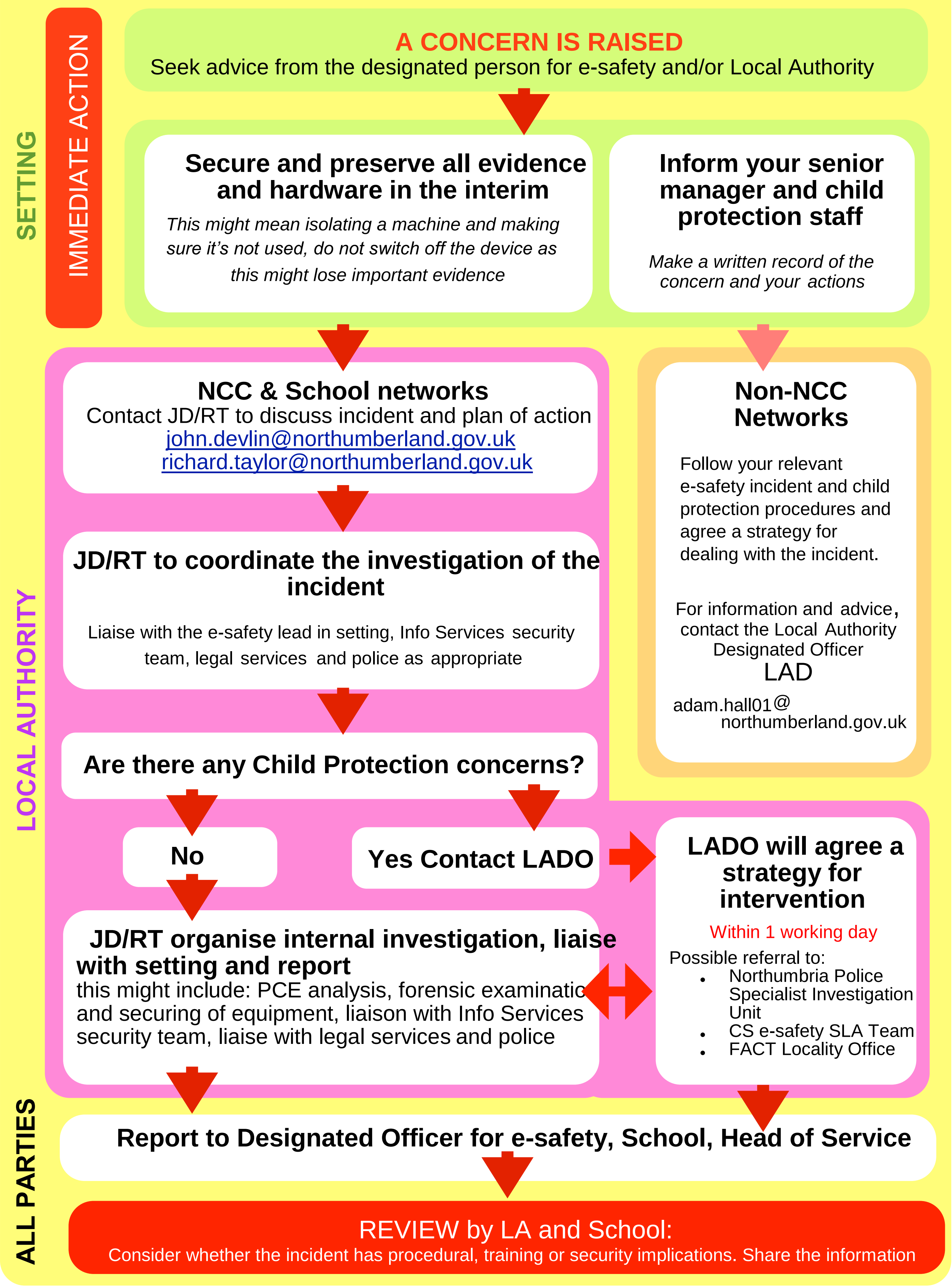
Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for Computing, Behaviour, Bullying and for Child Protection. It must be read in conjunction with the school's Acceptable Use Policies.

- The school's e-Safety Co-ordinators are Miss Abigail Evans, Computing Lead and Mrs Claire Gray, Head Teacher.
- The school governor with specific responsibility for computing and e-safety is Mrs Anna Ridley.
- Our e-Safety Policy has been written by the school, building on the SWgfl e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

Reviewed	September 2022
Approved by governors	
Review date	September 2023
Person Responsible for Implementation and Monitoring	Head Teacher Computing Lead

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

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

JD/RT organise internal investigation, liaise with setting and report
this might include: PCE analysis, forensic examinatio and securing of equipment, liaison with Info Services security team, liaise with legal services and police

Non-NCC Networks

Follow your relevant e-safety incident and child protection procedures and agree a strategy for dealing with the incident.

For information and advice, contact the Local Authority Designated Officer
LAD
adam.hall01@
northumberland.gov.uk

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

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