DE LACY
PONTEFRACT

De Lacy Primary School

E Safety Policy

2019 – 20

Date written:	September 2019
Next review date:	September 2020
Reviewed by:	Mrs Claire Hughes Mrs Gemma Smith

De Lacy Primary School E Safety Policy

At De Lacy Primary School we believe that all our children should aspire to be the very best they can. We pride ourselves on:

- Teaching fundamental skills in Literacy and Numeracy
- Providing stimulating first hand experiences
- Ensuring children experience a creative curriculum
- Developing essential skills for employment
- Developing a sense of what is right (set of morals)
- Ensuring children are thoughtful and aware of the needs for others
- Supporting children to become responsible citizens
- Fostering positive attitudes
- Recognising and developing individual strengths and talents
- Developing a sense of belonging to our school and wider community

E-Safety

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

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

Good Habits

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

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Yorkshire and Humberside Grid for Learning including the effective management of content filtering.
- National Education Network standards and specifications.

E-Safety Audit – Primary Schools

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with CYPD guidance?	
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Have school e-Safety Rules been set for pupils?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Has the school filtering policy has been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N

Contents

School e-Safety Policy

De Lacy Primary School will appoint an E-Safety coordinator. In many cases this will be the Designated Child Protection Officer as the roles overlap.

Our E-Safety Policy has been written by the school, building on the Government guidance. It has been agreed by the senior leadership team and approved by governors.

The E-Safety Policy will be reviewed annually. This policy will next be reviewed in November 2019. It will also be shared with new staff as part of induction and all staff at the start of each academic year (and at relevant points if required).

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access

Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- De Lacy's Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the Alamo helpdesk via the e-safety coordinator or network manager.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system.
- 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.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully.
- The forwarding of chain letters is not permitted.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- School social networking sites such as Twitter and Facebook are permitted to be accessed by staff to share notifications on the school's account.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location through E Safety and the curriculum
- Pupils will be taught through on going E safety how to keep themselves safe when using social networking.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

Managed ICT Service (Alamo): It is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff, as suggested below.

It is also important that the managed service provider is fully aware of the school e-safety policy and procedures.

The Managed ICT Service 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 Trust / other

relevant body ESafety 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
• the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
• 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 / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School / Senior Leader; E-Safety Coordinator for investigation / action / sanction
• that monitoring software / systems are implemented and updated as agreed in school policies

Video Conferencing (If appropriate)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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 are only to be used in adult areas E.G Office space and staff rooms
- Staff will be issued with a school phone where contact with pupils is required.

Mobile Phones

<u>Staff</u>

- Staff will be issued with a school phone on educational visits
- If personal phones must be used it must be out of sight of children
- Mobile phones must NEVER be used to take photographs of children
- Parents must not be contacted on personal mobile phones
- All personal phones and I Pads must be password protected

<u>Children</u>

- Mobile phones are not permitted in school
- If mobile phones are required after school time they must be handed to the office on a morning, clearly labelled at the owners risk

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Head of School or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Cameras

- Only school equipment may be used to photograph or video children
- Children will not be authorised to bring cameras into school or for trips
- Any adult helper on a trip or in school will not be permitted to bring cameras into school or on trips
- Any children that have left must be deleted
- Parents will be informed of the school procedure in relation to productions or celebrations via the home school agreement

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority / PAT

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR 2018

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school, the PAT nor Wakefield Council can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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 of School
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

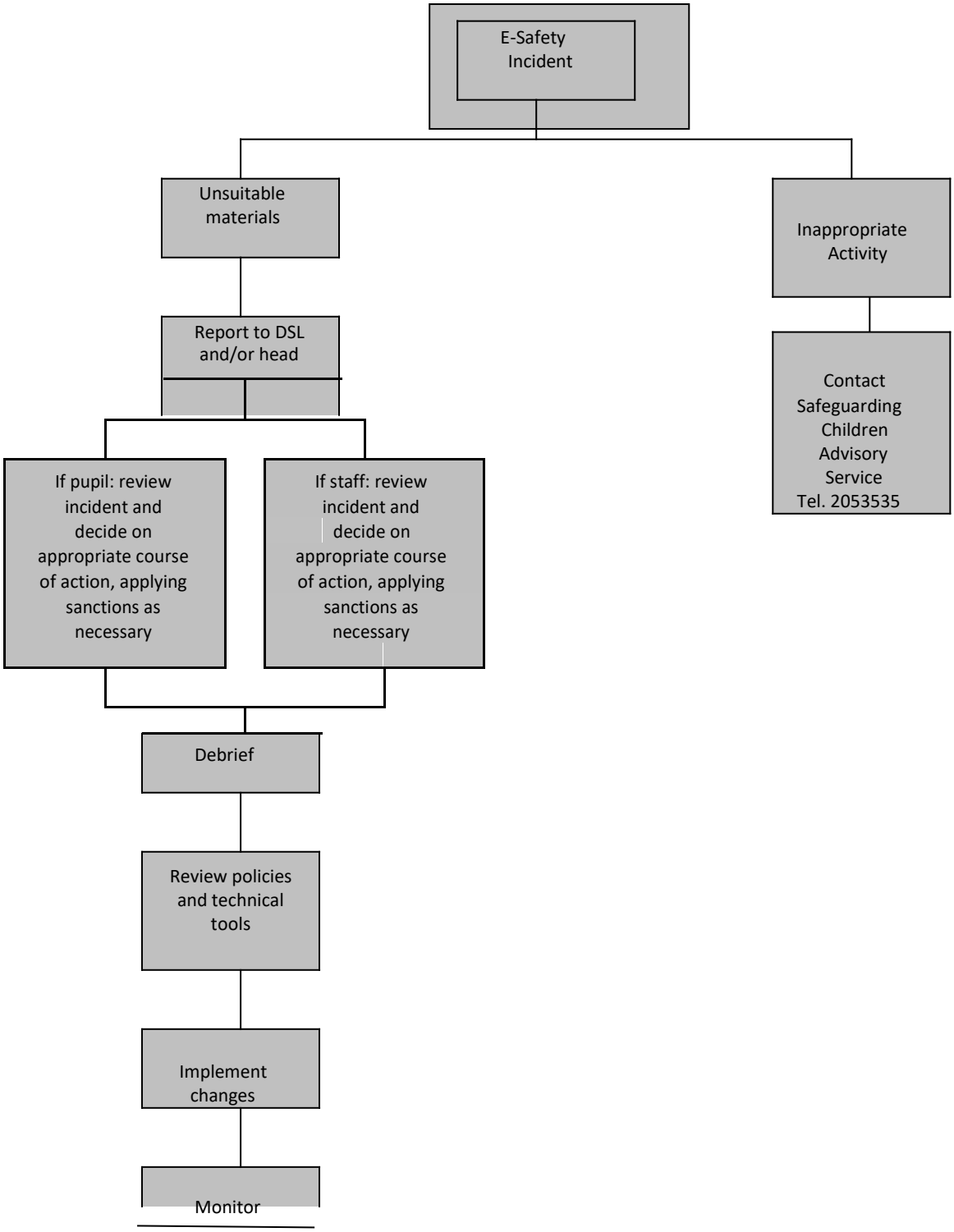
- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- Parents will sign a home-school agreement (See Appendix).

Appendix A

Flowchart for responding to e-safety incidents in school



Adapted from Becta – E-safety 2005

Appendix B

E-safety rules for Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

E-safety rules for Key Stage 2
Think then click!

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Rules for Responsible Internet Use at De Lacy Primary School

School has computers and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the Internet;
- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will not bring flash drives into school unless I have been given permission;
- I will only e-mail people I know, or my teacher has approved;
- The messages I send will be polite and sensible;
- I will not give my home address or telephone number, or arrange to meet someone;
- I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like (to help protect other pupils and myself);
- I will ask an adult if I am unsure if a website is reliable or if the information I am going to use is accurate;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I realise that if I use the Internet irresponsibly, access may be denied.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix C

De Lacy Primary School

E-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's consent for web publication of work and photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's consent for internet access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**
Please print name:	

Please complete, sign and return to the school

Appendix D
Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner
- I will ensure that my information systems use will always be compatible with my professional role
- I understand that school information systems may not be used for private purposes, without specific permission from the head teacher
- When using social networking sites, I will not have anything that links me to my personal role or breeches the Pontefract Academies Trust code of conduct
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager
- I will not install any software or hardware without permission
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely
- I will respect copyright and intellectual property rights
- I will always use encrypted (password protected) flash drives to store all school data and information
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator
- I will ensure that any electronic communications with pupils are compatible with my professional role
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create
- My mobile phone and I Pad will be password protected when in school

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct. My Signature in the Safeguarding Central file will act as my understanding of this Code of Conduct.

Appendix E

Dear Parent / Carer,

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. Staff may also show age appropriate clips from media as part of a lesson, from time to time these may be taken from PG films for junior classes. Images taken may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website, school Twitter account (more information to follow) and occasionally in the public media.

The school will comply with the Data Protection Act and requests parents / carers permission to take images of pupils at our school; as outlined above. We will also ensure that when images are published that pupils cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Yours Sincerely

Mrs Claire Hughes
Assistant Head Teacher / Designated Safeguarding Leader

Permission Form (please sign and tick)

Parent / Carers Name_____

Pupil(s) Name _____

☐ As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

☐ I agree that my child is allowed to view PG films when used as part of the curriculum and learning. **Years 3 to 6 ONLY**

Signed_____ Date_____