Valley Nursery School

E-Safety Policy

February 2020

Signed Governors: _____ (Finance Committee)
Date: 26th February 2020

E-Safety Policy

This policy refers to all technology use in Valley Nursery School, Little Chicks and applies to all children, students, staff, governors and families who use the setting.

The responsible member of staff for E-Safety is: Dawn Kelly

The designated Safeguard lead is: Dawn Kelly

The E-Safety Co-ordinator is: Liz Sledge

The governor responsible for E-Safety is: Nicola Davidson

E-Safety training and updates are provided for adults working within school.

This policy is reviewed by governors annually.

Please read this policy carefully as you will be deemed to be aware of its contents.

The purpose of this policy is to ensure that users of the school's equipment and services understand the way in which it is allowable to use the Internet. This policy aims to ensure that the Internet is used effectively for its intended purpose, without infringing legal requirements or creating unnecessary risk.

The policy applies to all users and administrators of the school's service and/or infrastructure when using the school's equipment and connections whether on the premises or elsewhere.

On evidence uncovered by the school, an employee may be disciplined. At the same time, if a user's conduct and/or action(s) are illegal the user may become personally liable in some circumstances.

The school encourages users to make effective use of the Internent. Such use should always be lawful and appropriate. It should not compromise the school's information and computer systems nor have the potential to damage the school's reputation.

Use of Internet Facilities

The school expects all users to use the Internet responsibly and strictly according to the following conditions: For the purpose of this document, Internet usage means any connection to the Internet via Web browsing, external email or other communication means. Users shall not:

- Visit Internet sites, make, post, download, upload, or pass on, material, remarks, proposals, or comments that contain or relate to:
    - Pornography (including images of children)
    - Promtoing discrimination of any kind
    - Promtoing racial or religious hatred
    - Promtoing illegal acts
    - Any other information or images which may be offensive to colleagues or have the potential to damage the school's reputation.

The school acknowledges that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use (for example investigating racial issues). Any such access should be pre-planned and recorded so that it can be justified if required.

- Incidents which appear to involve deliberate access to Web sites, newsgroups and online groups that contain the following material will be reported to the police:
    - Images of child abuse (images of children, apparently under eighteen years old) involved in sexual activity or posed to be sexually provocative.
    - Adult material that potentially breaches the Obscene Publications Act in the UK.
    - Criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to the school so that this can be taken into account in monitoring.

School employees must not:

- Use the school's facilities for running a private business.
- Enter into any personal transaction that involves the school.
- Visit sites that might be defamatory or incur liability on the part of the school or adversely impact on the image of the school.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials without written permission.
- Reveal or publicise confidential or proprietary information, which includes, but is not limited to: financial information, personal information, databases, and the information contained therein, computers/network access codes, and business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including (sending or receiving of large files or sending and receiving of large numbers of others in their use of the Internet.
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Gambling, or any gaming involving possible financial gain or loss.

Monitoring

The school will monitor and audit the use of the Internet to see whether users are complying with the policy. Any potential misuses identified by the school will be reported to the appropriate authorities and will be acted upon.

Teaching and Learning

Why the Internet and digital communications are important:

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils 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.
- Pupils will be taught what Internet use is acceptable and what is not. Pupils will also be given clear guidance when using the Internet.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access

Information system security

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

E-mail

- Pupils at Valley do not use email.

Published content and the school web site

- Staff or pupil contact information will not generally be published; the contact details given online should be the school office.
- The Head Teacher or their delegated representative will take overall editorial responsibility and ensure that content is accurate and appropriate.

Published pupil's image and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused, where suitable the school will use group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used anywhere on a school web site or other online space, 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 pupils and parents/carers.
- Pupils image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents/carers will be advised that the use of social network space outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking site.

Managing Filtering

- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.
- All community users will be required to have read and agreed to the school Acceptable Use Policy which applies to them.

Communications Policy

Staff and the E-Safety Policy

- All staff will be given the School E-Safety Policy and its importance explained.
- All staff will receive E-Safety training when they join the school.
- Staff must be informed that network and Internet traffic will be monitored and can be traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will publish a list of e-safety resources for parents/carers.
- The school will ask all new parents/carers to sign the parent/pupil agreement when they register their child with the school.

Appendix One: Useful resources for teachers

BBC Stay Safe	www.bbc.co.uk/cbbc/help/safesurfing/
Becta	http://schools.becta.org.uk/index.php?section=is
Chat Danger	www.chatdanger.com/
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Cyber Café	http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen	www.digizen.org/
Kidsmart	www.kidsmart.org.uk/
Think U Know	www.thinkuknow.co.uk/
Safer Children in the Digital World	www.dfes.gov.uk/byronreview/
WMNet	www.wmnet.org.uk/
Fetsafe Online	www.getsafeonline.org/

Appendix Two: Useful resources for parents/carers

Care for the family	www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
“Know It All” CD	publications.teachernet.gov.uk
Family Online Safe Institute	www.fosi.org/
Internet Watch Foundation	www.iwf.org.uk/
Parents Centre	www.parentscentre.gov.uk/
Internet Safety Zone	www.internetsafetyzone.com/
Getsafe Online	www.getsafeonline.org/
Think U Know	www.thinkuknow.co.uk/
BBC Say Safe	www.bbc.co.uk/cbbc/help/sagesurfing/

ICT Code of Conduct

The protocols in place for the use of ICT at Valley Nursery School are as follows:

Mobile Phones

- Mobile phones should not be located, seen or used in classrooms at any times by any staff, parents/carers, students or visitors.
- Staff visitors' phones should be left with staff personal belongings before each session.
- Mobile phones should not be used in staff rooms at Valley Nursery School or the Children's Centre.
- Mobile phones may be used at lunchtimes and afterschool, where children are not present and away from staffrooms.

iPads

- iPads may be used in classrooms for assessment purpose. Internet access **must** be switched off whilst in use in the classroom.
- iPads must be password protected. iPads must be kept in school at all times and stored securely at the end of each session.
- Children's use of iPads should be scrutinised and filtered for safety with safe programmes used. These should be monitored by staff.
- Learning Book tablets are permitted in School for assessments.

Cameras

- Cameras may be used in all classrooms or outdoor areas for the purpose of documenting children's learning.
- Cameras should never be taken into toilet areas.
- Photographs of children can be downloaded/printed etc. at PPA time.
- Parents/Carers **must** give consent for children's photographs to be used for publishing on Web sites, leaflets, newsletters or anywhere outside of school.

Laptops

Each member of staff is responsible for the safety and security of their Laptop. Laptops may be taken home but **must** be password protected. Laptops must **never** be left overnight in staff cars.
Laptops should not be used for personal use, Facebook, social networking sites,, personal email accounts. They are property of the school and should be used for school business only.

Whiteboards

Programmes used on Whiteboards in school should be closely monitored and the authority filtering processes should be applied. Internet access should be supervised. Internet access should be provided by the approved educational Internet service provider which complies with DFE requirements.