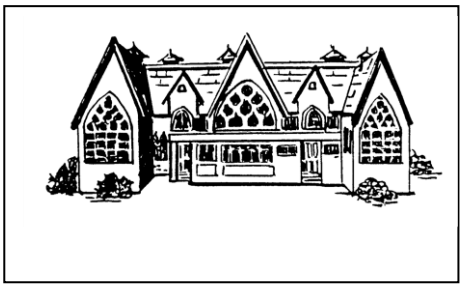

WEST VALE PRIMARY SCHOOL

E-SAFETY POLICY 2017

Introduction

Pupils interact with new technologies and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

E-safety covers issues relating to children and their use of the Internet, mobile phones and other electronic mobile devices, both in and out of school. It includes education on risks and responsibilities, the Prevent Strategy and is part of the 'duty of care' which applies to everyone working with children.

Who does this policy apply to?

This policy is relevant to all members of the school community who have access to and use school ICT systems both in and out of school.

Roles and responsibilities

The **Governors** are responsible for:

- Approving the e-safety policy and reviewing the effectiveness of the policy.

The **Headteacher/SLT** is responsible for:

- Ensuring the safety of all members of the school community.
- Take a lead role in day to day e-safety issues.
- Ensuring adequate CPD is provided on issues concerning e-safety within the school.
- Following procedures in the event of a serious e-safety allegation being made against/or concerning a member of staff or student within the school.
- Ensuring the school's commitment to the Prevent Strategy.

The **Computing co-ordinator** is responsible for:

- Ensuring e-safety is a standing item on the ICT agenda.
- Taking a lead role in day to day e-safety issues.
- Annually reviewing the e-safety policy of the school.
- Providing training within the school community on e-safety.
- Liaising with the Local Authority.
- Liaising with the Headteacher and SLT.
- Logging all e-safety incidents to help inform for future e-safety practices/developments.
- Attending relevant meetings where appropriate.

The **School Business Manager** is responsible for:

- Ensuring the school's infrastructure is secure and not open to misuse/attack.
- The school meeting the e-safety technical requirements as required.
- Remaining at the forefront of e-safety technical requirements as required.
- Ensuring data is held in line with the Data Protection Act 1998.

The **Teaching/Support staff** are responsible for:

- Having an up to date awareness of e-safety matters and the school policy.
- Implementing the Policy on Internet, Telephone, Photographs and E-mail usage for staff.
- Reporting any suspected misuse/problem to the ICT co-ordinator for investigation/action/sanction.
- Ensuring all digital communication (email, mobile phone text etc.) with students is on a professional level and carried out using only school systems.
- When using ICT, they reiterate to students the school e-safety policy/acceptable use policy and where there are breaches report through the relevant procedures.
- Ensuring that copyright law is abided by when using materials from the internet.

The **Child Protection Officer** is responsible for:

- Having an up to date awareness of e-safety matters.
- Having an up to date awareness of the potential risk for serious child protection issues such as:
    - Sharing of personal data
    - Access to illegal/inappropriate materials
    - Access to extremist viewpoints
    - Inappropriate contacts with strangers
    - Potential/actual grooming
    - Cyber bullying

The **Children** are responsible for:

- Ensuring they use school ICT systems appropriately following the school e-safety policy/acceptable use policy.
- Understanding how to report issues of abuse/misuse within school and know how to do so.
- Knowing and following school policy on the use of mobile phones, digital cameras and any other devices as well as the use of images appropriately.
- Understanding the importance of good e-safety practice when using digital technology both in and out of school.
- Ensure copyright is abided by when using information from the internet.

The **Parents/Carers** are responsible for:

- Ensuring their child understands the issues surrounding e-safety.
- Endorsing the child acceptable use policy. Please note children will not be given access to the school network until the acceptable use policy has been returned signed by both the child and parent.

Teaching and Learning

The purpose of the internet tool in school is to raise educational standards, promote children's achievement, support the professional work of staff and enhance school management functions.

Children at West Vale Primary School are encouraged to use the internet both within and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own security.

By allowing children and staff to use the internet we are opening up a vast resource of materials to support their learning and continuing professional development.

The school internet access is designed specifically for children's use and will include appropriate filtering for the age of the children. West Vale Primary School maintains a current record of all staff and children who are granted access on the computer network. Both staff and children must signthe acceptable use policy before being allowed access to the school internet, agreeing to comply with the e-safety rules. Parents will also be asked to sign a consent form for children's access.

Children will be taught what acceptable use of the ICT facilities is and given clear objectives or internet use. They will be made fully aware of the consequences of breaching these rules.

The school and individuals will ensure that copyright law is abided by when materials from the internet are used.

West Vale Primary School uses a filter system to block access to websites which promote extremist viewpoints, including the advocacy of violent extremism and terrorist materials. If staff or children discover unsuitable sites, these need to be reported to the ICT co-ordinator or the School Business Manager.

West Vale Primary School blocks all access to social networking sites for children and staff. Training will be provided to ensure all children are aware of the importance of not providing personal information that would allow another person to identify them/their location. Advice will be given to children on acceptable practice when using social networking sites outside of school. Staff **must not** allow children to access them personally through social networking sites.

The school will work with the relevant agencies to ensure that the systems to protect children and reviewed and improved. If staff or children discover unsuitable sites, these need to be reported to the ICT co-ordinator or School Business Manager.

Emerging technologies will be examined for educational benefit and a risk assessment carried out before use in school.

Managing Information Systems

The security of the school information systems will be reviewed regularly and virus protection will be updated regularly on the school system. Any data that is to be sent over the internet will be encrypted.

Any files on the school network will be checked regularly for security purposes. Unapproved files of executables will not be allowed in children's areas. Portable media may be used in the school but

only following a virus check to ensure they are not infected.

The school will take all reasonable precautions to ensure that users access only appropriate material. Due to the nature of the internet, it is not possible to guarantee access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or consequences resulting from internet use.

The use of the school network without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Personal data held on the school network will be recorded, processed, transferred and made available according to the Data Protection Act of 1998.

E-mail accounts

Children will only be able to use approved class email accounts. Should a child receive an inappropriate email they should report it to the teacher immediately who should then inform the Headteacher/SLT. In any email communication, children should not reveal personal information about themselves or arrange to meet a person unless they know the person. Access to external email accounts in school should be blocked.

All staff will have access to a school email account which will allow them to communicate with people outside of school. It is up to the member of staff to ensure that all communications re school is done so in a professional manner and using only school systems.

The School Website

The contact details on the website should be the school address, phone number and email address. Staff/children's personal information must not be published. The Headteacher is responsible for ensuring that all information on the school website is appropriate.

Written permission should be kept up to date and gained from parents, when children join the school. This is required before any images of students and placed on any communication for the school for that academic year, (This includes newsletters, letter, website etc.).

How to report an e-safety incident

Complaints of internet misuse will be dealt with by the Headteacher. Any complaint about staff misuse must be reported directly to the Headteacher.

Children, parents and staff will all be informed of the complaints procedure. It is expected that both children and parents will work to support the school should any issue arise.

Consequences to children that will be implemented by West Vale Primary School in the cases of misuse will include:

- Removal of privileges
- Parents/Carers being informed/invited into school to discuss the situation
- Removal of internet access for a given period
- Removal of network access for a given period
- School exclusion for a fixed period

Consequences to staff will be at the discretion of the Headteacher.

Communicating E-safety

Children

All classrooms will contain posters about e-safety and acceptable use of the internet and school computer network. Children will be informed that their network and internet activity is monitored. E-safety will be taught through PSHCE and ICT lessons. Internet safety week will be on the school calendar each year and assemblies for all year groups will take place during this time to promote e-safety.

Staff

All staff will be given the e-safety policy and its application and importance explained. Training on e-safety will be provided on a cycle annually.

Parents

Parents will receive information regarding e-safety through school newsletters and information sheets. The e-safety tab on the school website provides them with different websites which offer support for how their child can keep safe when using the internet.

A partnership approach with parents is to be encouraged with a display being made available throughout the year on e-safety at all events. Parents will be invited to a meeting to be held once per year to provide information on the latest developments on e-safety.

Reviewing this policy

This policy was written by the ICT co-ordinator. Consultation with the Headteacher, SLT. Governors, Staff and Parents will also take place. This policy will be reviewed by the Computing co-ordinator annually and any changes identified will be consulted to the SLT, Business manager, Governors and Staff.

July 2017

Signed

Headteacher _____

Presented to Governors_____

Signed

Chair of Curriculum