St Andrew's CE (VA) Infant and Junior School
working together in partnership for the future of our children

At St Andrew's, children will be taught to become reflective about beliefs and values, use their imagination and creativity to develop curiosity in their learning. They will be helped to develop and apply an understanding of right and wrong both in their school life and life outside school and be encouraged to take part in activities to develop their social skills. Children will develop an awareness of and respect for diversity in relation to gender, race, religion and disability. All pupils will have the same access to all areas of the curriculum regardless of their gender, race or cultural background.

E-Safety Policy

Rationale

We are committed to safeguarding and caring appropriately for every aspect of the lives of the children at both St Andrew's Infant School and St Andrew's Junior School. Together, we recognise our responsibility to take action on behalf of all children and others who are, or may be, at risk of neglect from physical, sexual or emotional abuse at the hands of any other person. The statutory curriculum expects pupils to learn how to locate, explore and exchange information using ICT. In delivering the curriculum, teachers need to plan for and make use of communications technology. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop ICT life skills to support this. The primary concern for teachers, with regard to the online environment, is the safe and effective supervision of pupils using the internet and educating pupils on what to do to avoid risk and report any internet abuse, by highlighting some of the associated risks and ways to deal with them, if encountered. We must not only protect pupils when they are in our care, we must also educate them to apply their understanding for when they work outside the school environment.

School Responsibilities

This policy has been developed in conjunction with the Calderdale Internet and E-mail Usage Policy and will be approved by Governors and reviewed annually. Each school has their own person responsible for e-Safety, this is the Designated Person for Child Protection (DPCP).

Teaching and Learning

Internet use is part of the statutory curriculum, a necessary tool for learning and an essential element in 21st century life for education, business and social interaction. At St Andrew's, children use the internet on a daily basis. The school has a duty to provide children with quality and safe Internet access as part of their learning experience via specific sites or using Google. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care for their own safety.

Internet Benefits in Education:

- 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
- 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 DfE
- Access to learning wherever and whenever convenient

To enhance learning: Pupils will be

- taught what Internet use is acceptable and what is not, and be given clear objectives for Internet use.
- educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Staff should guide pupils in on-line activities to support learning outcomes planned for the pupils' age and maturity.

How will pupils learn to evaluate Internet content?

As our pupils move into KS2 they will begin to use the Internet more widely outside school. We will encourage the children to evaluate on-line materials and to take care of their own safety and security, being aware of the CEOP report abuse button.

Managing Information Systems - Security of the school information systems

- The security of the school information systems will be reviewed annually by the IT Coordinator. Virus protection will be updated regularly by Compubyte/Calderdale IT and security strategies will be discussed with them.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media must not be used without first undergoing a virus scan.
- Compubyte/Calderdale IT manage our IT system and will review system capacity regularly.

Managing e-mail

Pupils will not have access to a school email account. Staff emails sent to external organisations on behalf of the school should be written carefully. The forwarding of chain letters is not permitted using school email addresses.

Managing Published Content

The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published. The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate. The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright. E-mail addresses should be published carefully, to avoid spam harvesting.

Publishing pupil images and/or work

Images that include pupils will be selected carefully to use on the school website/school Facebook page. A letter will be sent out when a child starts school assuming that this can take place unless a parent writes stating that they wish their child to be excluded from this.

Social networking and personal publishing

The YHGfL blocks access to all social networking sites in school.

Filtering

- The school's Internet filter will be provided by the LA in conjunction with YHGFL.
- If staff or pupils discover unsuitable sites, the URL must be reported to the IT Coordinator.
- Any material that the school believes is illegal must be reported to appropriate agencies such as YHGFL or CEOP by the Headteacher.

Emerging Technologies

- New technologies will be examined for educational benefit and a risk assessment will be carried out before such technologies are used in school.
- Children will not be allowed to have a mobile phone in their possession in school. The parents of some children in Y5 and Y6, who travel to school independently, may wish them to carry a mobile phone with them. However, it must be switched off and handed in to the teacher in charge of the class at the beginning of the day. It will then be given back at the end of the school day. Parents will be required to fill in a permission form. School will not be held responsible for any loss, theft or damage to phones.
- The school will investigate wireless communication technologies.

Personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- At the start of Reception, parents will be informed that pupils will be provided with supervised Internet access throughout their schooling at both St Andrew's Schools and will be asked to inform the Headteacher in writing if they do not wish their child to access the internet at school.

Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor YHGFL can accept liability for the material accessed, or any consequences resulting from Internet use.

E-Safety Complaints

Complaints about staff or children's Internet misuse will be referred to the Headteacher/Designated Person for Child Protection and the School's Complaints Procedure will be followed. All incidents will be recorded. All involved will be carefully questioned by the DPCP to understand the case, working in conjunction with the Local Authority Designated Officer (LADO) – ***Children's Social Care, Lower Valley Team: 01422 373491*** in extreme cases and reporting incidents to CEOP (Child Exploitation Online Protection) via the CEOP website: *www.ceop.police.uk*

Introducing the Policy to Pupils

• Basic e-safety children's training will be introduced to raise the awareness and importance of safe and responsible internet use throughout the year in every year group to ensure children know what to do to keep safe when using the internet. Instruction in responsible and safe use should precede Internet access. Rules for using the internet will be posted near computers and explained to the children.

Parents' Support

Parents' attention will be drawn to the school's e-safety policy. Internet issues will be handled sensitively, and parents will be advised accordingly.

Consultation, Monitoring and Review

This policy will be reviewed annually to ensure adequacy and appropriateness. Any changes made based on the review will be documented and all staff informed.

Policy written: July 2013 by Nicola Martin.
Consultation with staff and parents/carers: July 2013
Reviewed by Karen Smith and Karen Cotterill: September 2015

Rules for Responsible Internet Use

St Andrew's Infant School and St Andrew's Junior School have computers with Internet access to help our learning. These rules will keep you safe and help us to be fair to others.

☺ I will log-in with my own name and password (which I will keep secret).

☺ I will not access other people's files.

☺ I will only use the computers for school work and homework.

☺ I will not bring CDs or memory sticks in to use from outside school unless I have been given permission.

☺ If I see anything bad on the computer, I will tell an adult straightaway.

☺ I will only email people I know, or that my teacher has approved.

☺ The messages I send will be polite and responsible.

☺ I will not give my home address or telephone number, or arrange to meet someone via the internet or messaging.

☺ I will report any unpleasant material or messages sent to me. I understand this will be confidential and will help to protect other pupils and myself.

☺ I understand that the school may check my computer files and may monitor the Internet sites I visit.

By following these rules, we want you to stay safe. For anyone found to be breaking these rules, the school's behaviour procedures will be followed.

Staff Acceptable Use of Information Systems

It is a requirement that members of staff sign this code of conduct. They may wish to consult the school's e-safety policy and ICT Code of Practice for further information and clarification.

- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will report any incidents of concern regarding children's safety to the e-safety co-ordinator, the Designated Person for Child Protection.
- I will promote e-safety with the children in my care and will help them to develop a responsible attitude to system use, communications and publishing.

RED – Unacceptable Use

- DO NOT knowingly, view, send or receive material, which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress.
- DO NOT use the Internet and e-mail facilities for personal purposes in works time, UNLESS usage is in compliance with the Green – Acceptable Use section below.
- DO NOT use e-mail to engage in gossip.
- DO NOT make libellous statements about individuals or other organisations.
- DO NOT make statements purporting to represent the school when they are personal views.
- DO NOT make derogatory remarks or express derogatory opinions regarding the school.
- DO NOT knowingly infringe copyright or intellectual property rights.
- DO NOT knowingly use the facilities for any activity, which is illegal or fraudulent.
- DO NOT use the facility to pursue personal business interests, for gambling or for political purposes not directly related to your job.
- DO NOT allow anyone else to use your Internet access or e-mail account or provide any other person with the means to access these facilities by disclosing your user ID and password etc.
- DO NOT knowingly engage in any activity, which threatens the integrity or availability of the school's systems.
- DO NOT attempt to gain unauthorised access to (hack) any server/facility whether inside or outside the school.
- DO NOT install any unauthorised programs, such as screen savers on the school's information assets.
- DO NOT open junk emails in school.

GREEN – Acceptable Use

- YOU MAY use the Internet and e-mail facilities in school for work purposes.
- YOU MAY use the Internet and e-mail facilities for personal purposes outside work time.
- YOU MAY open personal e-mails received in your school e-mail account in works time.
- YOU MAY use the facilities, with the prior approval of the Headteacher, for personal purposes in work time.

Where e-mail is stated, this means your school e-mail account – it does not refer to personal web based e-mail accounts. These are treated as 'internet and e-mail facilities'.

The use of computer systems for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and could result in disciplinary action.

Social Networking and Mobile Phones Code of Conduct

- It is essential that we apply the utmost care if we run a **public** or **private** Facebook account. There can be no public postings which could bring our school name into disrepute. Public postings and content should be in keeping with the Christian School ethos.

Private Networking

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend'
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18. Where family and friends have pupils in school and there are legitimate family links, please inform the Headteacher in writing.
- Employees should not identify themselves as a representative of the school.
- References should not be made to any staff member, pupil, parent or school activity /event unless prior permission has been obtained and agreed with the Headteacher .
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.
- It is illegal for an adult to network, giving their age and status as a child.
- If you have any evidence of pupils or adults using social networking sites in the working day, please inform the Headteacher.
- No pupil under 13 should be accessing social networking sites.

Public Networking (e.g. school Facebook account)

- Postings must be in keeping with our school ethos.
- Pictures must be appropriate and permission must be obtained from parents or members of staff involved.
- Inappropriate comments must be investigated and deleted.
- Postings must be consistent with other school literature and publications.

Mobile Phones

The following rules apply for the use of personal mobile phones:

- Children are not permitted to bring mobile phones to school.
- As a general rule, employees are not permitted to make/receive calls/texts during work time (excluding break times)
- Staff should ensure that mobile phones are turned off/ on silent at all times while on school premises.
- They should be kept in a locker or bag and not be left on display.
- In the event that an employee has a particular reason for a specified period of time, they may request via the SMT that they leave their phone on during working hours.
- Staff are not permitted to use recording equipment on their personal mobile phones, for example: to take photographs or videos of children.

I agree to abide by these guidelines set out above:

Name:

Signature: Date: