



St Aidan's Primary School  
A Church of England Academy

## **St. Aidan's Primary School-A Church of England Academy**

### **Online Safety Policy- Revised January 2017**

#### **Using new learning technologies effectively and safely**

Technology is commonplace and its effective use is an essential life skill. Unmediated access to a range of resources brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. A policy is required to help ensure acceptable use were the safety of pupils and staff is safe guarded.

Online safety depends on staff, school governors, advisors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. St. Aidan's Primary School Acceptable Use Policies intend to address all aspects of responsible internet use by both adult and child user and state clearly what the expectations and responsibilities of all users are. As communication technologies develop we anticipate reviewing and where necessary amending our policies accordingly for the benefit of all users.

Governors, staff, community groups, and visiting tutors requesting access to our network should sign a copy of the Acceptable Policy and return it to the Headteacher. Children will have their responsibilities explained and made clear to them and the Acceptable Use statements will be clearly displayed in all areas of school. The children will have the expectation that technology is for learning and the understanding that the rules are there to protect them and be adhered to. Through clear Online safety lessons and discussions in each class throughout the year children will be reminded of the consequences of the misuse of technology. We will encourage the children to understand that Online safety is a priority at home as well as school and that if they follow the basic rules of responsible use then the Internet is a very positive tool crossing all boundaries of race, religion gender and class.

## Scope

This policy applies to all members of St. Aidan's Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school's ICT systems. The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

<u>Role</u>	<u>Key Responsibilities</u>
<u>Headteacher</u>	<p>To take overall responsibility for online safety provision</p> <ul style="list-style-type: none"><li>• To take overall responsibility for data and data security</li><li>• To ensure the school uses an approved, filtered Internet Service, (Light Speed) which complies with current statutory requirements</li><li>• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant</li><li>• To be aware of procedures to be followed in the event of a serious Online safety incident.</li><li>• To receive regular monitoring reports from the Online safety Coordinator</li><li>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures( e.g. network manager)</li></ul>
<b>Online safety Coordinator Online Safety Group /</b>	<ul style="list-style-type: none"><li>• Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies</li></ul>

<p><b>Designated Child Protection Lead</b></p>	<p>documents promotes an awareness and commitment to e-safeguarding throughout the school community</p> <ul style="list-style-type: none"> <li>• ensures that online safety education is embedded across the curriculum</li> <li>• liaises with school ICT technical staff</li> <li>• To communicate regularly with SLT and the designated online safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident</li> <li>• To ensure that an online safety incident log is kept up to date</li> <li>• facilitates training and advice for all staff</li> <li>• liaises with the Local Authority and relevant agencies</li> <li>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: sharing of personal data</li> <li>• access to illegal / inappropriate materials</li> <li>• inappropriate on-line contact with adults / strangers</li> <li>• potential or actual incidents of grooming</li> <li>• cyber-bullying and use of social media</li> </ul>
<p><b><u>Governors / Online safety governor</u></b></p>	<p>To ensure that the school follows all current online safety advice to keep the children and staff safe</p> <ul style="list-style-type: none"> <li>• To approve the Online safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online safety Governor</li> <li>• To support the school in encouraging parents and the wider community to become engaged in online safety activities</li> </ul>
<p><b><u>Computing Curriculum Leader</u></b></p>	<p>To oversee the delivery of the online safety element of the Computing curriculum</p> <ul style="list-style-type: none"> <li>• To liaise with the online safety coordinator regularly</li> </ul>

<p><b><u>Network Manager/technician</u></b></p>	<p>To report any online safety related issues that arises, to the online safety coordinator.</p> <ul style="list-style-type: none"> <li>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)</li> <li>• To ensure the security of the school ICT system</li> <li>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>• the school's policy on web filtering is applied and updated on a regular basis</li> <li>• that he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant</li> <li>• that the use of the network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher for investigation / action / sanction</li> <li>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>• To keep up-to-date documentation of the school's e-security and technical procedures</li> </ul>
<p><b><u>Data Manager</u></b></p>	<p>To ensure that all data held on pupils on the school office machines have appropriate access controls in place</p>
<p><b><u>Teachers</u></b></p>	<p>To embed online safety issues in all aspects of the curriculum and other school activities</p> <ul style="list-style-type: none"> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)</li> </ul>

	<ul style="list-style-type: none"> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</li> </ul>
<b><u>All staff</u></b>	<p>To read, understand and help promote the school's online safety policies and guidance</p> <ul style="list-style-type: none"> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy</li> <li>• To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices</li> <li>• To report any suspected misuse or problem to the online safety coordinator</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through CPD</li> <li>• To model safe, responsible and professional behaviours in their own use of technology</li> <li>• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.</li> </ul>
<b><u>Pupils</u></b>	<p>Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)</p> <ul style="list-style-type: none"> <li>• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>• to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• To know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school policy on the taking / use of images and on cyber-bullying.</li> <li>• To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety</li> </ul>

	<p>Policy covers their actions out of school, if related to their membership of the school</p> <ul style="list-style-type: none"> <li>• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> <li>• to help the school in the creation/ review of online safety policies</li> </ul>
<b><u>Parents/carers</u></b>	<ul style="list-style-type: none"> <li>• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images</li> <li>• to read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>• To access the school website on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement.</li> <li>• to consult with the school if they have any concerns about their children's use of technology</li> </ul>
<b><u>External groups</u></b>	<p>Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school</p>

### **Writing and reviewing the online safety policy**

The online safety Policy is part of the School Development Plan and relates to other policies including those for computing, bullying and for child protection.

- Mrs. Harrison is the schools Online safety coordinator who works in collaboration with the child protection coordinator.
- Our online safety Policy has been written by the school, building on the Blackburn with Darwen amended version of the Kent online safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The online safety Policy and its implementation will be reviewed annually or in response to an incident.

## **Safety Audit**

This quick self-audit will help the senior management team (SMT) assess whether the online safety basics are in place to support a range of activities that might include those detailed within Appendix 1.

Has the school an online safety Policy that complies with Becta 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 Coordinator is:	
The online safety Coordinator is:	
Has online safety training been provided for both students and staff?	
Do all staff sign an ICT Code of Conduct on appointment?	
Do parents sign and return an agreement that their child will comply with the School online safety Rules?	
Have school online safety Rules been set for students?	
Are these Rules displayed in all rooms with computers?	
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access	
Has an ICT security audit been initiated by SMT, possibly using external expertise?	
Is personal data collected, stored and used according to the principles of the Data Protection Act?	

## **Teaching and learning**

As the children's access and understanding expands, so should the guidance and rules to ensure safe access use of the internet.

### **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.

### **Pupils will be taught how to evaluate Internet content appropriate to their age.**

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is responsible 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 appropriate to their age group.
- Sanctions for inappropriate use of the internet will be explained to the children.
- 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 computing systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Security strategies will be discussed with Blackburn with Darwen.

## **Managing filtering**

- The school will work with the LA, DCSF 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 head and Online safety Coordinator and the LA will be informed so that they can take appropriate action.

## **Staying safe**

The school will ensure that pupils and parents are aware of online safety issues. A list of useful addresses and resources is included in this document and on our website.

- The school internet access is designed expressly for pupil use and includes appropriate filtering.
- Pupils may only use approved digital methods of communication on the school system e.g. not forwarding chain letters.
- Pupils will be taught to tell an adult immediately about any offensive communications they receive or any inappropriate content they may encounter using digital technology.
- Pupils and staff will use equipment responsibly.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location or arrange to meet anyone without specific permission.
- Pupils and parents will be advised that the unsupervised use of social network spaces outside school is inappropriate for pupils.

## **Published content**

Any information that can be accessed outside the school's intranet should be classed as published whether in electronic or paper format.

- Electronic communication 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.
- General contact details should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

## **Publishing pupil's images and work**

- Staff and pupils using digital cameras, video recorders or sound recorders will ensure that they inform others before recording them and always use equipment in a respectful manner.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Written permission from parents or carers will be obtained before photographs or video of pupils are published.

## **Managing emerging technologies**

- The educational benefit of emerging technologies and any potential risks will be considered before it is used in school.

## **Protecting personal data**

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

## **Policy Decisions**

### **Authorising Internet access**

- All staff must read and sign the 'Acceptable Use Policy' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Parents will be asked to sign and return a consent form.

### **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 Blackburn with Darwen LA can accept

liability for the material accessed, or any consequences of Internet access. Any inappropriate access whether intentional or unintentional will be reported to the online safety coordinator and to the LA where necessary.

- The school will audit ICT provision to establish if the online safety policy is adequate and that its implementation is effective.

### **Handling online safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff and where appropriate inform the LA.
- Any complaint about staff misuse must be referred to the headteacher.
- 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 on request.

### **Communications Policy**

#### **Introducing the online safety policy to pupils**

- Online safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. This will begin in Reception through to Year 6.
- Pupils will be informed that network and Internet use will be monitored and can be monitored and traced to the individual device or login.

#### **Staff and the online safety policy**

- All staff will be given the School online safety Policy and its importance explained through the planning and implementation of an Online safety week and staff meetings when required.
- Staff should be aware that internet traffic may be monitored and traced to the individual device or login. Discretion and professional conduct is essential.

- The school may use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

### **Enlisting parents' support**

- Parents' attention will be drawn to the School online safety policy in newsletters, the school website, use of the schools social media pages and through workshops / meetings.

Kelly Harrison

Date of policy: Revised January 2017

Approved by the Local Governing Board: To be approved

Review Date: