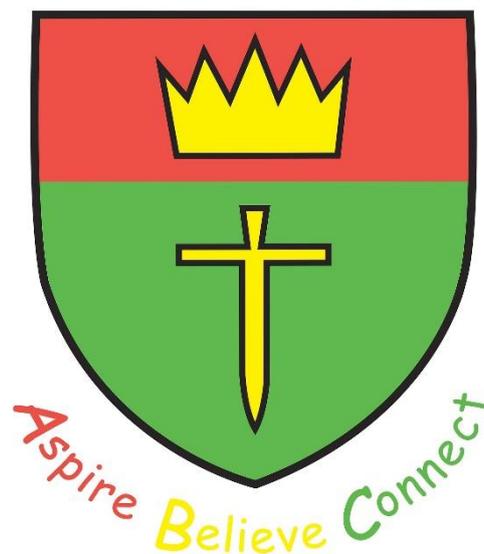


# St Oswald's CE VA Primary School

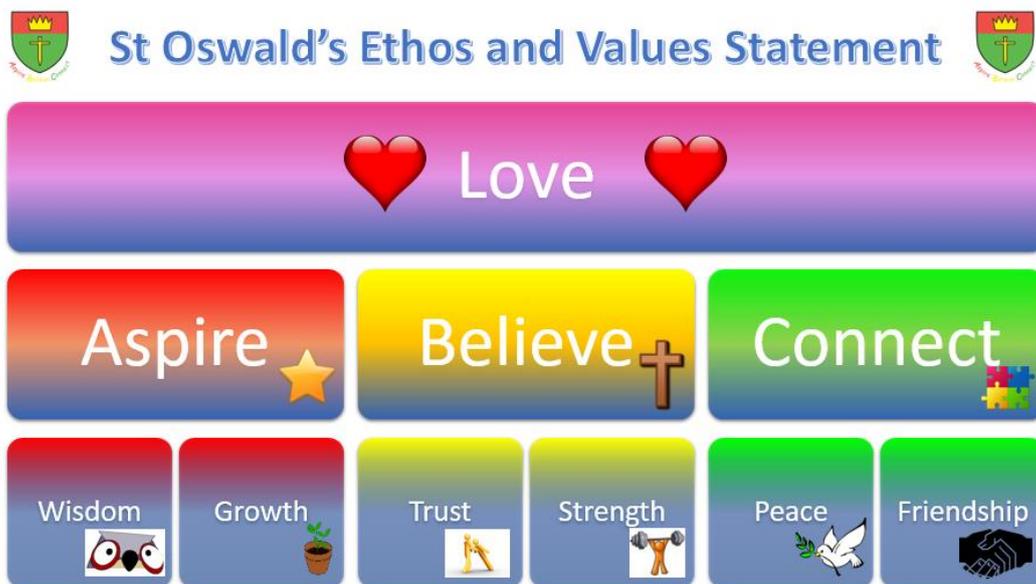


## E-Safety and Acceptable Use Policy



## E-safety and Acceptable Use Policy St. Oswald's C of E Primary School

### Ethos and Values Statement



### *Background*

Our Ethos and Values Statement underpins everything we do at St Oswald's CE VA Primary School. Children in our school know that love is the most important value of all, in line with the new command that Jesus gave us to love one another, which is why this is placed above all in our statement.

### *Mission Statement*

Sitting below love lies our school's mission statement: *Aspire, Believe, Connect*. As easy as A, B, C, this statement is easy to remember and most importantly represents what we want our children to do in every aspect of their education and lives.

### *Core Christian Values*

The mission statement is underpinned by six core Christian values that each link to one aspect of *Aspire, Believe, Connect*. As children aspire to be the best they can be in every way, they will grow in wisdom. In order to believe in themselves and develop their own beliefs about the world around them, our children are taught about the importance of trust and strength on their journey. We also believe in the values of peace and friendship in helping us to connect with those around us.

### **E-safety and Acceptable Use**

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.

Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these

Internet technologies and that some have minimum age requirements (13 years in most cases).

At St Oswald's CE VA Primary School, we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

### **Monitoring**

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

All internet activity is logged by the school's internet provider. These logs may be monitored by that provider, Durham Net (as of February 2017).

### **Breaches**

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

A breach of the Acceptable Use policy by a child, will result in procedures set out in the school's Behaviour Policy being followed.

### **Incident Reporting**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows:

Mrs Helen Smith (Head Teacher)

Mrs Ali Conway (Computing Lead)

Mr Mark Tulip (ICT Technician)

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Mrs Helen Smith, or Mrs Ali Conway. Additionally, all security breaches, lost/stolen equipment or data virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

A record of e-safety incidents helps us to monitor and identify trends or specific concerns.

### **Internet Access**

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the ADVANTEX internet service is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites, online services, software and apps before use
- Searching for images through open search engines is discouraged when working with pupils unless using a child safe search engine.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be

advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other source.
- All users must observe copyright of materials from electronic resources

### **Internet Use**

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

### **Safe Use of Images**

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the School App
- on the school's social media sites (Facebook and Twitter)
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Members of the Senior Management Team are permitted to post the school website and social media sites.

### **Storage of Images**

- Images/ films of children are stored on the school's network in a secure area called Photoshare

- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- Ali Conway and Helen Smith have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

---

### **Mobile Technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

#### ***Personal Mobile Devices (including phones)***

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device
- Pupils are allowed to bring personal mobile devices/phones to school but must be given to a member of staff as soon as they enter school. It will be returned to them at the time of dismissal.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed

#### **Social Media and School App**

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter and the school App to communicate with parents and carers. The Senior Management team and the Office Manager are responsible for all postings on these technologies and monitors responses from others
- Pupils are unable to access their social media accounts whilst at school
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

Disclaimer

St. Oswald's School in conjunction with ADVANTEX will endeavour, wherever possible, to provide a safe and secure environment for its users. However, users must be aware that we cannot guarantee complete safety from inappropriate or illegal material.

I agree to abide by the conditions set out in this policy

\_\_\_\_\_ (signed)

\_\_\_\_\_ (print name)

Policy review date: Spring 2019



## Acceptable Use Agreement: Pupils

- I will only use ICT in school for school purposes
- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not sign up to online services until I am old enough

Name of child: \_\_\_\_\_ Signed by child: \_\_\_\_\_

Name of parent: \_\_\_\_\_ Signed by parent: \_\_\_\_\_

Date: \_\_\_\_\_



Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Ali Conway (ICT and Computing Lead).

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂-----

**Parent/ carer signature**

We have discussed this document with .....(child's name)  
and we agree to follow the eSafety rules and to support the safe use of ICT at  
St Oswald's Church of England Primary School.

Parent/ Carer Signature .....

Class ..... Date .....



## Staff, Governor and Visitor

### Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs Helen Smith.

- I will only use the school's email / Internet/ social media accounts and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Mrs Helen Smith
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices (including smart watches) in public areas of the school between the hours of 8.30am and 3.30pm.

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

## **E-safety and Acceptable Use Policy**

Signed: *Ali Conway*

Date completed: June 2017

Effective date: July 2017

Date of review: June 2019