"*Let your light shine*" **Matthew 5:16**

Governor Policy 49 - E-Safety, Mobile Technology and ICT Acceptable Use Policy

- **Policy adopted and agreed: November 2019**
- **Review undertaken by: Headteacher and Safeguarding Governor**
- **Policy Review Period: Annual**
- **This revision: November 2020**

E-Safety Policy

E-Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school is committed to safeguarding its pupils and as such, this policy should be read in conjunction with other relevant policies including our Safeguarding policies; Behaviour, Anti –Bullying and Social Networking policies

Good Habits

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from the South West Grid for Learning including the effective management of content filtering.

The school's ICT Co-ordinator acts as our E-Safety co-ordinator.

Our E-Safety Policy has been agreed by the staff and approved by governors.

The E-Safety Policy will be reviewed annually.

Why is Internet Use Important?

The purpose of internet use in school is:

- To raise educational standards, to promote pupil achievement
- To support the professional work of staff
- To enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality internet access.

Pupils will use the internet outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

- Benefits of using the internet in education include:
- 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
- Access to experts in many fields for pupils and staff
- 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 the Local Authority and DfE; access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted internet access
- All staff must read the 'Social Media Policy' before using any school ICT resource
- Parents are informed that pupils will be provided with supervised internet access
- Permission is sought each year through the Home School Agreement for children to use the internet responsibly in relation to their studies.

World Wide Web

- If staff or pupils discover unsuitable sites, when possible, the URL time, content and computer should be recorded and reported to the E-safety co-ordinator who will ensure that the information is passed on to SWGfL. Parents of children involved should be informed, usually by the class teacher, detailing the school's response
- The school will ensure that the use of internet derived materials by pupils and staff complies with copyright law
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Pupils may only use approved e-mail accounts on the school system, once this facility becomes available
- Pupils must immediately tell a teacher if they receive offensive e-mail(s)
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Watches

For safeguarding reasons, watches that connect to the internet, or use wi-fi to phone, message and have video or camera or voice recording facilities, are not allowed in school.

Mobile Phones

Staff Use: (this means school staff, volunteers and governors)

- The school allows staff to bring in personal mobiles phones and devices for their own use.
- Staff are advised to use passwords/pin-codes to ensure their device cannot be used by an unauthorised person.
- There should be no personal use of mobile devices during student contact time, phones should be 'invisible' to the pupils.
- In exceptional circumstances, e.g. family emergency, staff should seek permission from Headteacher / Deputy to use their personal mobile device when in contact with students.
- Staff should not give their personal mobile phone numbers or personal email addresses to students, parents or carers.
- Only the mobile devices belonging to school may be used to take appropriate and relevant images of students, e.g. for observations, school events. Personal mobile devices should not be used.
- Staff bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- During off site visits, staff will be provided, where possible, with a school mobile phone and this should be used to contact school or parents should an emergency arise. However, if a school mobile device is not available then staff can use their personal mobile device with authorisation from a member of SLT and in this instance should block their number when calling.

Pupil Use:

- There should be no need for pupils to bring a mobile phone into school. However, if parents seek prior permission from staff, giving good reason for a pupil to have a phone in school, it may be kept in the school office until collection at the end of the day.
- Pupils who ignore this policy and use a mobile device on school premises will be required to hand over their device to a member of staff. Parents will be contacted to inform them that this has happened and asked to collect the device from the school office.
- If a member of staff of the school has any suspicion that a mobile device has unsuitable material stored on it, pupils will be required to hand over the device to a member of staff and parents will be asked to collect it from a senior member of staff. In circumstances where there is a suspicion that material on the device may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation. Parents will need to recover the device from the police in such circumstances.
- Mobile technology must not be used to share inappropriate or offensive imagery or messages at any time. Emergencies:
- If parents need to contact pupils they should contact the school and a message will be relayed promptly.

Visitor Use:

- Visitors should not use their personal mobile devices in the school building. These should be turned off whilst in school.
- Parents/carers are permitted to take photos/videos during assemblies or other school performances that involve their own children. They are reminded not to place photographs or videos showing other children on Facebook or other social media platforms.
- School Photographers will be treated as any other visitor and appropriate levels of supervision will be in place at all times.

Staff and Volunteer Social Media

- Pupils are advised not to use social networking sites
- We encourage pupils and parents to discuss use of the internet at home and raise awareness of cyberbullying

- Social networking is not permitted on school equipment and social networking sites and newsgroups are blocked by the school's filter
- Pupils are advised never to give out personal details of any kind which may identify them or their location
- Pupils are advised not to place personal photos on any social network space
- The school has a Social Networking Policy; all staff are asked to read and sign in agreement of its terms.

Cyber Bullying

Cyber bullying is any form of bullying which takes place online or through smartphones and tablets. There are many ways of bullying someone online and for some, it can take shape in more ways than one. Some of the types of cyber bullying are:

Harassment - This is the act of sending offensive, rude, and insulting messages and being abusive.

Denigration – This is when someone may send information about another person that is fake, damaging and untrue. Sharing photos of someone for the purpose to ridicule, spreading fake rumours and gossip.

Outing and Trickery – This is when someone may share personal information about another or trick someone into revealing secrets and forward it to others. They may also do this with private images and videos too.

Cyber Stalking – This is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages or engaging in other online activities that make a person afraid for his or her safety.

Exclusion – This is when others intentionally leave someone out of a group such as group messages, online apps, gaming sites and other online engagement. This is also a form of social bullying and very common.

The school will educate pupils, parents and staff about the prevalence and dangers of cyberbullying through assemblies, newsletters and in ICT lessons.

Any report of cyberbullying involving school pupils or staff will be treated in accordance with the school Anti Bullying Policy.

Sexual Imagery

All incidents involving pupil produced sexual imagery will be responded to in line with the school's safeguarding and child protection policy.

When an incident involving pupil produced sexual imagery comes to the school's attention:

- The incident should be referred to the DSL as soon as possible
- The DSL should hold an initial review meeting with appropriate school staff
- There should be subsequent interviews with the young people involved (if appropriate)
- Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm
- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to MASH/or the police immediately

If the school receives a disclosure of sexual imagery of a pupil which involves an adult, an immediate referral is to be made to the police.

Filtering
The school will work in partnership with the Local Authority, Becta and the Internet Service Provider such as South West Grid for Learning (SWGfL) to ensure filtering systems are as effective as possible.

Video Conferencing

- Video conferencing will only ever take place under direct supervision from a member of staff (normally Class Teacher or TA.)

Published Content and the School Web Site

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

Publishing Pupils' Images and Work

- Pupils' full names will not be used anywhere on the website particularly in association with photographs
- Children are only referred to using their first names on our website and these are not explicitly published with their names
- Only use images of pupils in suitable dress to reduce the risk of inappropriate use of images of pupils

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection is installed and updated regularly by the school's ICT support technician
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

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

Assessing Risks

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- All Saints Primary School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither All Saints Primary School nor Dorset County Council can accept liability for the material accessed, or any consequences of internet access.
- The school should audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a senior member of staff

- Any complaint about staff misuse must be referred to the headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school 'Child Protection' policy and procedures
- Pupils and parents will be informed of the complaints procedure.

Communication of Policy

Pupils

- Rules for E-Safety are to be located near the computers in each classroom.
- Pupils are informed that internet use can be monitored.

Staff

All staff will be given the School E-Safety Policy and its importance explained.
Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- The E-Safety policy will be available for parents on the school's website or in hard copy upon request.