E-Safety Policy – St Saviour's Catholic Primary School

Rationale

At St Saviour's we recognise that new technologies have become an integral part of today's society, both within schools and in everyday life. In accordance with our Mission Statement, we strive to develop respectful, 'confident and independent citizens' who recognise the benefits and limitations of using the internet and other digital and information outlets.

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.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school, are expected to adhere to the schools Acceptable Use Agreement and this e-safety policy.

Complaints or concerns relating to e-safety should be reported to the Designated Safeguarding Lead, who will liaise with the e-safety coordinator where appropriate.

E-safety in the curriculum

At St Saviour's the teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and learn to take responsibility when using a range of technologies. Children are educated on how to seek help or advice if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button. These actions also apply to any incidents of cyber bullying.

We follow Switched On Computing from FS2 to year 6 to deliver the computing curriculum which embeds and emphasises the importance of e-safety. Some of the apps and software we currently use within school are:

- Websites
- Coding
- Video and Multimedia
- Mapping
- Email
- Twitter
- Gaming

As a school, each year, we also participate in e-safety activities during Safer Internet Day.

E-safety guidelines and the SMART rules are displayed around the school.

Security, Data and Confidentiality

All new users and staff must read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the School Data Protection Regulations 2018 which reflects the General Data Protection Regulations 2018.

All parents/carers are asked to agree to and sign a Home School Agreement at the beginning of each academic year which includes reference to the E-Safety Policy.

Infrastructure and security

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. Filtering software is provided by the LA, which will block/ filter access to social networking sites. We will seek advice from the Local Authority with regard to technical matters relating to system security. If staff or pupils discover an unsuitable site, it must be reported to the Safeguarding Lead, who is known to all members of the school community.

School ICT systems and security will be reviewed regularly.

Virus protection will be installed on every computer and will be set to update automatically.

Mobile Technologies

Personal mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use when in the staff room at appropriate times. These are not to be used at any time whilst children are present unless in extreme circumstances e.g. emergencies, educational visits, etc...
Any personal mobile devices do not have access to the internet via the school's WiFi network.

Pupils who walk home in years 5 and 6 are permitted to bring their mobile phones into school under the written permission of their parents/carer. These will be stored by the class teacher in stock rooms during the school day.

Music devices (without internet access) are permitted to be used as part of curriculum enhancement.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing emails

The use of email within school is an essential means of communication for staff. Staff must use the school's approved email system for any school business. Staff must inform a senior leader if they receive an offensive or inappropriate e-mail.

Pupils are not permitted to access individual email accounts within school.

Social Networking

All teachers have access to the school's Twitter account which may only be used for school purposes.

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day. (These sites are currently blocked by the LA.)

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which have a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

With the written consent of parents/carers (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. 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.
All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions to publish on a public domain.
Any photographs published will not include names.
Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes educational visits. School's own mobile devices must be used in this case.

Whilst we cannot control the use of parents/carers own personal devices, we remind all parents/carers to not upload any images/films taken.

During educational visits, adult helpers are not permitted to use any personal mobile devices to take images and all helpers will be referred to the 'guidance card' (see appendix 1).

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops/IPads.

Inappropriate materials

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Safeguarding Lead.

Deliberate access to inappropriate materials noticed by any member of staff must be immediately reported to senior management. Depending on the seriousness of the offence; investigation maybe carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Conclusion

Through application of this policy, we aim to educate and protect both our pupils and staff whilst providing a technology-rich and inspiring curriculum.

February 2019