KING'S STANLEY C OF E PRIMARY SCHOOL

WHERE WE CARE ABOUT LEARNING AND EACH OTHER

King's Stanley C of E Primary School E-safety Policy
Written by: Mr van den Broek
Reviewed: December 2024,

Introduction

At King's Stanley Primary School, we believe that learning about and how to use computers and computing is central to all aspects of learning, for adults and children in both the school and the wider community. This policy reflects updates in technology and online safeguarding requirements to ensure it remains relevant in a rapidly evolving digital landscape.

ICT in the 21st Century is 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, we aim to embed the use of these technologies to prepare our young people with the skills to navigate lifelong learning, employment, and online safety.

All children, whatever their needs, will have access to a range of up-to-date technologies at school. ICT is a life skill and should not be taught in isolation.

Information and Communications Technology and the computing curriculum covers a wide range of resources including web based. It is also important to recognise the constant and fast paced evolution of using computers within our society. Currently the internet technologies children are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Streaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At King's Stanley 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 are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach… Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'
(Becta Safeguarding Children Online Feb 2009)

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

Whole school approach

All members of the school community have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

The computing leader will ensure they are up to date with current guidance and issues through organisations such as Gloucestershire LA, Becta, CEOP (Child Exploitation and Online Protection), SWGFL advice and Child Net.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. In 2024, we have expanded our approach by integrating new tools, such as updated e-safety lessons using the latest SCARF curriculum materials.

- Pupils are taught about the **importance of critical digital literacy skills**, including identifying fake news, misinformation, and responsible content sharing.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people they do not know

Managing Internet Access

In 2024, the school has enhanced its filtering and monitoring system with the latest Securus update, offering improved reporting capabilities for staff and DSLs (Designated Safeguarding Leads). Children will have supervised access to Internet resources

- Staff must continue to preview recommended sites and discourage raw image searches.

- Raw image searches are discouraged when working with pupils. Staff must continue to preview recommended sites and discourage raw image searches. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
- Our internet access is controlled through the SWGFL web filtering service.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to an ICT leader, technician or member of SLT.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up to date on all school machines.

E-mail

The use of email within school is an essential means of communication for staff. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school, between schools or international. We recognise that pupils need to understand how to style an email in relation to their age.

- Pupils are introduced to email as part of the Computer Science Scheme of Work.
- The school gives staff their own email account, to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils will not normally need to use email. However, if they do, they may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- The forwarding of chain letters is not permitted in school.
- Staff must inform a member of SLT if they receive an offensive e-mail.

- Staff must continue to preview recommended sites and discourage raw image searches.

Publishing pupil's images and work

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

- on the school web site
- 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
- Social media appearances, e.g. Twitter/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Pupils' names will not be published alongside their image and vice versa without permission from the parents. Full names will not be published.

Social networking and personal publishing

We block/filter access for pupils and staff to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils

- Pupils and parents are reminded that children under the age of 13 are not permitted on many social platforms, such as Instagram and TikTok, without breaching terms and conditions.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- All classes have been issued with an iPad to use for school photography, assessment notes, emails, music and educational applications.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

- Data can only be accessed and used on school computers. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data. **Data Protection Act 2018**

  Overview

  This Act makes provision about the processing of personal data.

  Most processing of personal data is subject to the GDPR (General Data Protection Regulation).
  Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply (see Chapter
  https://www.legislation.gov.uk/ukpga/2018/12/section/1/enacted

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to ESafety should be made to a member of the senior leadership team. Any complaint about staff misuse must be referred to the Headteacher.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Headteacher/

LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of computers and computing, particularly mobile phones and the internet, to deliberately upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Headteachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site.

Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying, these are listed in Appendix 2.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on www.kidscape.org and www.wiredsafety.org.

See appendix 7 & 8 for Key Safety Advice for children, parents and carers

Investigating Incidents

All bullying incidents should be recorded and investigated in an incident log as any other bullying incident. We will then investigate fully as any other bullying incident (refer to behaviour policy)

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"*It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure*

that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

- The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours
- Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility
- The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.
- Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced e.g. using SWGfL Test Filtering

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users: This is Securus monitoring system.

- The school monitors all network use across all its devices and services.

- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:
    - physical monitoring (adult supervision in the classroom)
    - internet use is logged, regularly monitored and reviewed
    - pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
    - where possible, school staff regularly monitor and record the activity of users on the school technical systems
    - use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Reviewing this Policy

There will be an on-going opportunity for staff to discuss with SLT any issue of safety that concerns them.

This policy will be reviewed every 24 months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.