Sir William Burrough School

E-Safety Policy

Introduction
Our e-safety policy has been written by the school, building on government guidance and other example policies and documents. It has been discussed with staff, agreed by the senior management and approved by Governors. The e-safety policy and implementation will be reviewed annually.

Context and background
ICT in the 21st century has an all-encompassing role within the lives of children and adults. Technology provides new learning opportunities – online collaboration, anytime-anywhere learning and communication – but at the same time can provide additional opportunities for students to access material they shouldn't, or be treated by others inappropriately. We should also be aware that children use technology widely outside of school and need to learn how to take care of their own safety and security. Our e-safety education is about ensuring the children are able to make the right decisions when they are online.

Managing Information Systems:
School Internet Provision
Internet services are provided through LGfL by Virgin Media Business.

Content Filter
The school works very hard to ensure that inappropriate material cannot be accessed from the internet. LGfL has web filtering in place to ensure that inappropriate content cannot be accessed at school. There is also a second layer of web filtering provided by OpenDNS. The security of the school information systems will be reviewed regularly. There are still circumstances when unsuitable material may get past the filter and the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet. Children are taught to immediately report any inappropriate material to an adult.

Published content and school website
The contact details on the Web site are the school address, e-mail and telephone number. Staff or pupils' personal information will not be published. The Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate. The school website has a dedicated e-safety page with links to pages that can support children and parents when they are online.

Downloading Applications
Children are not able to install applications from the internet or download apps from the app store on iPads. All hardware is managed by the network administrator.

Cloud Computing
The school gives children access to Google Apps for Education (GAfE). The children are advised that their accounts are monitored at all times by staff. GAfE has conducted its own DfE self-certification with regards to data protection.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Managing videoconferencing
Where pupils use videoconferencing technologies, they will be supervised at all times.

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

E-safety for pupils:
Use of the Internet by pupils
Children should be made aware of the positive role the internet and online services can take in education. Internet access is carefully controlled by teachers according to the age and experience of the pupils and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the internet, and computers with internet access are carefully located so that screens can be seen at all times by all who pass by.

Access for all pupils
In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the internet, particularly where this will directly support their learning.

Teaching safe use of the internet and ICT
- Teachers carefully plan all internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials and websites.
- Children are taught how to use search engines and how to evaluate internet-based information.

- Children are taught how to check the validity of information obtained online.
- Children are taught to keep their personal information private.
- Children are made aware of their online reputation and how they can be portrayed online.
- Children are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

We think it is crucial to teach pupils how to use the internet safely, both at school and at home, and we use the Kidsmart safety code (www.kidsmart.org) to support our teaching in this area. The main aspects of this approach include the following five SMART tips:

- Safe - Staying safe involves being careful and not giving out your name, address, mobile phone number, school name or password to people online.
- Meeting - Someone you meet in cyberspace can be dangerous. Only do so with the permission of your parent/carer and when they are present.
- Accepting e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.
- Remember someone online may be lying and not be who they say they are. If you feel uncomfortable when chatting or messaging, end the conversation.
- Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

These SMART guidelines are displayed in classrooms, the ICT suite and on laptop and iPad trolleys. Small logos are also on all pieces of technology as a reminder to children of the SMART guidelines.

Social networking, blogs and chat sites

These forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas. Online chat rooms, discussion forums, blogs and social networking sites present a range of personal safety and privacy issues for young people. Children are taught how to stay safe when using these sites out of school and how to report incidences where they feel uncomfortable. All commercial Instant Messaging and Social Networking sites are inaccessible on school premises. Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities.

Cyber bullying

Any incidences where bullying is taking place online will be dealt with in accordance with the school behaviour and child protection policies.

E-safety complaints

Children are taught to report anything they are unhappy about to an adult. Serious issues are then reported to the headteacher.

Introducing e-safety to pupils

The use of the internet and associated technology is discussed with children at the start of the year. Further teaching will take place throughout the year as children access more resources online.

Staff and e-safety

All staff will be given the school E-Safety Policy and receive annual training in e-safety. Any issues will be reported to the network administrator or headteacher.

Acceptable Use Agreement

All parents are required to sign the school acceptable use agreement.

Digital Leaders

Digital leaders are in place across KS2 to support children and look after class equipment. These children will help to lead discussion and inform staff and other children in the areas of e-safety.

Use of the internet and technology resources by staff:

Internet Availability

To enable staff to make full use of these important resources, the internet is available in school to all staff for professional use.

ICT Equipment and Resources

The school offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

Professional use

Staff are expected to model appropriate ICT and internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or training in using ICT as part of their professional practice can ask for support from the ICT co-ordinator.

Parent Permission Form

Child's name: …….

Child's Class: …….

As the parent/carer of the above pupil I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that all children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of acceptable behavior using these technologies.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed: ……

Date: ……..