Springbank Academy

Character Education Values

Courtesy-Forgiveness-Determination-Self-Discipline-Gratitude-Honesty

Our whole school vision is:
Springbank Academy is a place where all of our children and staff will have the opportunity to excel. Everyone will be safe, happy and cared for. Our curriculum and values will inspire everyone in the school family to be motivated and curious learners and offer core skills, knowledge and enrichment to enable all to gain the foundations for a quality future and a love for life-long learning.

In all we do we remember our school motto:

Caring-Happy-Healthy-Sporty-Scientific

School Values

Sportsmanship-Tolerance- Appreciation- Respect-Friendship-Integrity-Sensitivity-Helpfulness

E-Safety Policy

October 2021

Policy Lead: Hannah Clarke

Link Governor: Sara Dunn

Springbank Academy is committed to equal opportunities for all. It is our aim that every policy is written to have a positive impact on every child/all children irrespective of race; religion; gender; sexual orientation or age.

Springbank = success for all
There is a key that unlocks every child's learning, our job is to find that key.

Every staff member and governor must take the responsibility and accountability to ensure the procedures within this policy are delivered and implemented as per Springbank Academy Policy.

Springbank Academy E-safety Policy

Policy development

The e-safety policy relates to other policies including those for ICT, Anti-bullying and Safeguarding children.

- Our policy has been written with consultation from staff in school, parents/carers, governors and young people.
- It is reviewed annually by leadership and approved by governors.
- It is available to read or download on our school website or as a hard copy from the school office.

Roles and responsibilities

The school has an e-safety lead. Our IT Lead is: Hannah Clarke.

Teaching and Learning

Why internet and digital communications are important

- The purpose of any technology in school is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon or the Hector Protector function.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.
- Weekly E-Safety Assemblies are currently held virtually to reiterate the importance of staying safe on all technologies.

Managing Internet Access

Information security system

- The school ICT system security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies may be discussed with the Local Authority and at the annual DfE conference.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a member of staff if they receive offensive e-mails.
- Staff to pupil e-mail communication must only take place via a school e-mail address.
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Pupils will use their school Google email to sign into Google Classroom.

Published content and the school website

- The contact details on the school's website should be the school address. No staff or pupil's personal details will be published.
- Julie Vaccari, Dawn Wigley or Hannah Clarke will have overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified.
- Pupil's full names will be avoided on the website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission on the annual GDPR form will be obtained from parents and carers before any photographs are published on the school website.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites and consider how to educate pupils in their safe use. This may not mean blocking every site; it may need monitoring and educating students in their use.
- The school will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The school will work with the IT Consultant to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material will be reported to the e-safety lead.
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.

Managing video conferencing

- Video conferencing will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a video conference call.
- Video conferencing will use the educational broadband network to ensure quality of service and security.

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time except as part of an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required.

Protecting personal data

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

Policy decisions

Authorising internet access

- All staff must read and sign the 'staff code of conduct before using any school ICT resource.
- Parents will be asked to sign and return GDPR a consent form each year.
- At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff/complaint governor.
- Complaints of misuse by staff will be referred to the Head teacher.
- Any complaints of a child protection nature will be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the school's behaviour policy.

Community use of the internet

- All use of the school internet connection by community and other organisations shall be in accordance with the e-safety policy.

The Legal Framework

Communications Act 2003(section 127)

Sending by means of the internet a message or other matter that is offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction to imprisonment.

NB an offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990

Regardless of an individual's motivation, the act makes it a criminal offence to:

 Gain access to computer files or software without permission
 Gain unauthorised access as above in order to commit a further criminal act
 Impair the operation of a computer or program (for example caused by viruses or denial of service attacks)

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission.
Data Protection Act 1998
The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data.
Education Act 2011 (sections 2-4)
This clarifies statutory powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. Details for free schools can be found in section 36 and Academies in part 6 sections 55-65.
Education and Inspections Act 2006 (sections 90-91)
This provides powers to discipline pupils for inappropriate behaviour or for not following instructions both on and off the school premises. It also gives schools the powers to confiscate items from pupils.
These powers are particularly relevant to online bullying and e-safety as well as giving legal powers to confiscate mobile phones and other mobile devices, if they suspect that they are being used to compromise the well-being and safety of others.
Malicious Communications Act 1988 (section1)
This makes it a criminal offence to send electronic messages that conveys indecent, grossly offensive, threatening material or information that is false. This includes if the message is of an indecent or grossly offensive nature and if the purpose was to cause a recipient to suffer distress or anxiety.
Obscene Publications Act 1959 and 1964 (section 1)
Publishing an 'obscene' article is a criminal offence. This includes electronic transmission.
Public Order Act 1986 (sections 17-29)
This makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. It also makes the possession of inflammatory material with a view of releasing it a criminal offence. 21

Protection of Children Act 1978 (section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the UK. A child is anyone under 18. Viewing an indecent image of a child on your computer means that you have made a digital image.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which they know or ought to know amounts to the harassment of others. A person whose course of conduct causes another to fear on at least 2 occasions, that violence will be used against them is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear on each of these occasions.

The Equality Act 2010
This consolidates discrimination law covering all types of discrimination that are unlawful. It defines that schools cannot unlawfully discriminate against pupils because of their sex, race, disability, religion or belief and sexual orientation. Protection is now extended to pupils who are pregnant or undergoing gender reassignment.

Regulation of Investigatory Powers Act 2000
This regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication.
The Telecommunications (Lawful Business Practice) (Interception of Communications Regulations 2000) does permit a degree of monitoring and record keeping for example in schools to investigate unauthorised use of the network. However, all monitoring is subject to consent.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice and intentionally meet them or travel with the intent to meet them to commit a sexual offence.
Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.
It is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust.