E-SAFETY POLICY
2016

Believe and achieve

Salisbury Primary School's diverse community is a place where all children flourish in a safe, happy and stimulating environment.

E-Safety Policy
The e-safety officer for the school is the Head teacher.
Our e-safety policy recognises that measures must be in place in order to ensure Technology is used safely within all areas of learning and teaching. All reasonable steps are taken in order to safeguard our children and ourselves.

Virus Protection:
Only software with a site-licence that has been purchased by the school or the Local Authority is allowed to be used on the school premises.
Pupils are not allowed to bring private software disks or removable storage devices into school and, in particular "arcade" games software is banned. If found in school they will be confiscated and sent to the ICT manager, who will scan them for viruses and check if any breach of copyright has been made. In such cases, the ICT manager will report to the head who will decide on the appropriate action to be taken. If children bring in CD Rooms relating to their work, these will be used at the teacher's discretion.
Staff using removable storage devices must ensure that their home PC / laptop has Adequate virus protection (regularly updated and scanned) to safeguard the school network when transferring data. If a virus has been detected on external PC systems then the removable storage devices MUST not be used within the school. Emailing files to school from a system with a known virus can seriously damage the school network and must not be carried out in any circumstances.

Pupils who need to bring in work from home systems should email (with staff permission) as they are not permitted to bring in any removable storage devices. Virus protection software is installed on all networked computers. This software will be updated regularly according to the procedures set by the technician who will check that this has been completed. LA advice to protect the school from specific viruses will be taken. Staff (using laptops on home ISP) need to ensure that laptops are updated and scanned regularly and must notify the technician if a virus has been detected.
Staff must take every precaution to ensure the safety of school systems, their own pcs and laptops with regard to virus protection and internet security.

Unauthorised Access:
All personal, confidential and sensitive information will be protected by password restricted to authorised personnel only and will only be stored on a removable storage device if it is absolutely essential. When a removable storage device does contain confidential data, it will be stored in a locked safe or secure area

Software Router: LgFL
• Web guards protect the children from banned and unacceptable web sites.
• Lists of banned sites will be updated as appropriate.
• The router shall be securely locked away.
• Logging in passwords and other codes should not be divulged to the pupils.
• Pupils should not have access to logging in codes or other information related to the school systems.

Protecting Pupils from on line risks:
Introducing children to positive use of technology at an early age is important to ensure that they remain safe and aware of potential dangers and correct use of modern technology. Over the course of their learning within the school, teachers ensure that all age appropriate aspects of e- safety are covered with the pupils. Lessons around e-safety are explicitly delivered. Pupils learn about safe use of a range of modern technologies and as new advice is circulated from the LEA relevant year groups will be updated.

Reviewed by Governors on: 3rd December 2016

Next Review: December 2017