E Safety Policy

Approved:	**September 2017**
To be reviewed:	**September 2018**
Reviewed:	**October 2018**
Reviewed:	**October 2020**
To be reviewed:	**October 2022**

Introduction

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety.

Writing and reviewing the e-Safety policy

The school has a designated e-safety co-ordinator, Sarah Orr, who is also a member of the Safeguarding Team.
The e-Safety policy has been agreed by the senior management team and approved by the governors. It will be reviewed on an annual basis.

Safeguarding:
At Willen Primary School, safeguarding and child protection is paramount and we are fully committed to ensuring the welfare and safety of all our children. We believe that pupils have a right to learn in a supportive, caring and safe environment which includes the right to protection from all types of abuse; where staff are vigilant for signs of any student in distress and are confident about applying the processes to avert and alleviate any such problems. If any behaviour is a concern in relation to safeguarding Willen Primary School procedures and processes will be followed at all times in accordance with the Child Protection Policy. Any concerns will be referred to the Designated Safeguarding Leads; Sarah Orr, Carrie Mathews, Kim Cole, or Hayley Gates as procedures state.

Teaching and Learning

The purpose of internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the internet is a necessary tool for staff and students.
It helps to prepare students for their on-going career and personal development needs.
Computing is a requirement of the 2014 National Curriculum and plays a valuable contribution to other subject areas.
The school ensures that all children have age appropriate e-safety lessons as early as possible in each academic year, and that the rules and procedures outlined are revisited regularly.

Internet use enhances learning
Internet access is provided by Spitfire. This is designed expressly for pupil use and includes filtering appropriate to Primary age pupils. Filtering is provided through a secure GEA network with a Fortigate filter managed by our ICT partners, Partnership Education.

Internet access is planned to enrich and extend learning activities.

Access levels are reviewed to reflect the curriculum requirement.

Pupils are given clear objectives for internet use and sign a Pupil's Computer and Internet agreement.

Staff select sites which support the learning outcomes planned for pupils' age and maturity.

Pupils are taught how to take responsibility for their own internet access.

Pupils are taught how to evaluate internet content
Pupils are taught ways to validate information before accepting that it is necessarily accurate.

Pupils are taught to acknowledge the source of information, when using internet material for their own use.

Pupils are made aware that the writer of an e-mail or the author of a Web page might not be the person claimed.

Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing internet access

Information System Security
Virus protection is updated regularly and this is regularly monitored by Partnership Education .

E-mail
When being taught how to use email pupils learn that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
Pupils are taught not to open suspicious incoming email or attachments.
The forwarding of chain letters is not permitted.

Published content and the school web site
The website complies with the school's guidelines for publications.
All material must be the author's own work or where permission to reproduce has been obtained, it is clearly marked with the copyright owner's name.

Publishing pupils' images and work
Children's photographs are only allowed to go on the website once permission has been received from the child's parents. Children's work may be celebrated and shared on the website, but individuals will not be identified.

Social networking and personal publishing
Pupils will not be allowed to access public chat rooms without supervision.
They will be taught the dangers of using these 'chat rooms'.

Managing filtering
Internet access is provided by Spitfire. This is designed expressly for pupil use and includes filtering appropriate to Primary age pupils. Filtering is provided through a secure GEA network with a Fortigate filter managed by our ICT partners, Partnership Education.

The Fortigate filter is configured to block potential exposure to harmful material including those in the 'Potentially Liable' category, including material that would fall into the definitions of the PREVENT initiative.

Details can be found at www.fortiguard.com/static/webfiltering.html

As part of the monitoring cycle the SLT ensure that occasional checks are made to ensure that the filtering methods selected are effective in practice.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to Partnership Education (the ICT maintenance team) who will then investigate further and block access to these site if needed.

Managing emerging technologies
Mobile phones must not be used by children in school. The sending of abusive or inappropriate text messages is forbidden.
Only school cameras are used by both staff and children for educational purposes.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and March 2018 GDPR Regulations.
Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected. Staff are responsible for ensuring that their personal USB devices are security scanned regularly.
Children should not bring in USB devices.

Policy Decisions

Authorising internet access

All staff must read and sign that they have read the "Staff code of conduct " before using any school ICT source as this contains reference to ICT equipment.
The school maintains a record of all staff and children who have access to the school's ICT systems.
Parents are asked to sign a consent form regarding their child's internet use .

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network.
Neither the school, nor Spitfire can accept liability for any material accessed, or any consequences of internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling e-safety complaints

Complaints of internet misuse by children must be referred to the ICT Leader in the first instance who will liaise with the safeguarding Team and Partnership Education.
Any complaint about staff misuse must be referred to the Headteacher.
Complaints of a child protection nature must be dealt with in accordance with the school's child protection policy.
Pupils and parents are informed of the complaint's procedure.

Communications Policy

Introducing the e-safety policy to pupils

The schools E-safety rules are displayed on every netbook trolley and in various areas of the school, so all users can see them.
The children receive e-safety lessons early in each school year and are constantly reminded of online safety.

Staff and the e-safety policy

All staff are trained regularly and receive a copy of the E-safety policy.
Staff are informed that network and internet traffic can be traced to an individual user.

Enlisting parents' and carers' support

Parents' and carers' attention is drawn to the school's E-safety Policy in newsletters and on the school website. The website includes information and advice for parents about e-safety.