



## WILSON PRIMARY SCHOOL E Safety Policy

November 2017  
Review date November 2018

### 1. Introduction

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using media and information resources is one the school shares with parents and carers. Safeguarding is a serious matter; at Wilson Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

For clarity, the e-safety policy uses the following terms unless otherwise stated:

**Users** - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

**Parents** – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

**School** – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

**Wider school community** – pupils, all staff, governing body, parents, any groups using the school facilities.

This policy is available for anybody to read on the Wilson Primary School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff ICT Code of Conduct.

### 2. Roles and Responsibilities

#### Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

## **Headteacher**

Reporting to the governing body, the Headteacher has overall responsibility for safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties
- All e-safety incidents are dealt with promptly and appropriately.

## **e-Safety Officer**

The day-to-day duty of e-Safety Officers is devolved to MrsLeyland and Class teachers

The e-Safety Officers will:

- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use
- Review this policy regularly and bring any matters to the attention of the Headteacher
- Advise the Headteacher, governing body on all e-safety matters
- Engage with parents and the school community on e-safety matters at school and/or at home
- Liaise with the local authority, IT technical support and other agencies as required
- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail
- Ensure any technical e-safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or IT Technical Support
- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

## **IT Technical Support**

Technical Support Provider manage the server and all technical aspects within the school.

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum: anti virus, up to date operating system, appropriate internet filtering and passwords applied correctly

## **All Staff**

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher
- Any e-safety incident is reported to the e-Safety Officer (and a safeguarding report is made) or in his/her absence to the Headteacher.
- They sign the ICT Code of Conduct on joining the school as part of the Induction. This is kept in their HR file.

## All Students

The boundaries of use of ICT equipment and services in this school are given in the student Code of Conduct; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

E-safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

## Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and letters the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents and pupils will sign the Pupil ICT Code of Conduct before any access can be granted to school ICT equipment or services.

## 3. Technology

Wilson Primary School uses a range of devices including PCs, laptops, iPads and fizzbooks. In order to safeguard the student and in order to prevent loss of personal data we ensure the following measures are in place:

**Internet Filtering** – to prevent unauthorised access to illegal or inappropriate websites. Appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner.

**Email Filtering** – to prevent any infected emails being sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

**Encryption** – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an unencrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

**Passwords** – staff will only be able to access school devices with a unique username and password. Staff passwords will change on a yearly basis or if there has been a compromise, whichever is sooner.

**Anti-Virus** – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The IT Technical Support Provider will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

## 4. Safe Use

**Internet** – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this E safety Policy and the staff ICT code of conduct; students upon signing and returning their acceptance of the Pupil ICT Code of Conduct.

**Email** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

**Photos and videos** – All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance. Each class will have a list of those children whose photographs and videos cannot be put on the school website or blog sites. Children's full names are not displayed, first name only to be used.

**Social Networking** – The Wilson Primary School Blog is a networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following Blogging rules are to be strictly adhered to:

- Permission slips must be consulted before any image or video of any child is uploaded, these will be completed on a yearly basis
- There is to be no identification of students using first name and surname; first name only is to be used
- Where services are "comment enabled", comments are to be set to "moderated"
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

**Notice and take down policy** – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

**Incidents** - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer(s), or in his/her absence the Headteacher. The e-Safety Officer(s) will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

**Training and Curriculum** - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Wilson Primary School will have an annual programme of training which is suitable to the audience.

E-safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

Wilson Primary School will use the National Curriculum in Key Stage 2, to teach children about the importance of e-safety. Children in Key Stage 1 will be introduced to the important aspects of e-safety through role play and discussion with adults in the classroom. All children will learn about staying safe and wider safeguarding issues through the SRE scheme of work and where appropriate external professionals will also support this delivery.

## 5. Staff Declaration

I ..... confirm that I have read and understood the  
(print name)

E-Safety Policy.

Signed .....date.....

.....

**E-Safety Policy approved by Chair of Governors**

**Signed ..... date.....**

**Review Date .....**