**Willoughby Primary School**

**Willoughby Primary**

**School**

***‘Learning for Life’***



**E-Safety and Acceptable Use Policy**

**September 2021**

**Willoughby Primary School**

 **E-Safety Policy**

**Introduction**

Willoughby Primary School believes that it is the right of every person to be loved, respected and protected from harm. We recognise and take seriously our responsibility for safeguarding and protecting children, and this includes the children’s safety when using the internet and electronic devices. E-safety is a priority across all areas of school and is not specific to computing lessons.

E-safety is about the safety issues associated with information systems and electronic communications as a whole. This encompasses not only the internet but all wireless electronic communications including mobile phones, games consoles, cameras and webcams. It also needs to take into account the increasing mobility of access to digital technology through the range of mobile devices.

**Legal Framework**

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

* Voyeurism (Offences) Act 2019.
* The General Data Protection Regulation (GDPR).
* Data Protection Act 2018.
* DfE (2021) ‘Keeping children safe in education’.
* DfE (2019) ‘Teaching online safety in school’.
* DfE (2018) ‘Searching, screening and confiscation’.
* National Cyber Security Centre (2017) ‘Cyber Security: Small Business Guide’.
* UK Council for Child Internet Safety ‘Education for a Connected World’.
* UK Council for Child Internet Safety (2017) ‘Sexting in schools and colleges: Responding to incidents and safeguarding young people’.

This policy operates in conjunction with the following school policies:

* Acceptable Use Agreement.
* Child Protection and Safeguarding Policy.
* Anti-Bullying Policy.
* PSHE Policy / RSE Policy.
* Staff Code of Conduct.
* Behavioural Policy.
* Disciplinary Policy and Procedures.
* Data Protection Policy.
* Confidential Reporting and Whistleblowing Policy.

**Roles and Responsibilities**

**Governors**

Governors are responsible for ensuring that the school has an appropriate policy in place and that procedures are being followed.

**Head Teacher**

The head teacher has a duty of care for ensuring the safety (including online safety) of members of the school community.

**Network Manager**

The Network is managed by FrogBox. They are responsible for ensuring that:

* The school’s technical infrastructure is secure and is not open to misuse or malicious attack.
* The school meets required online safety technical requirements for any Local Authority/other relevant body’s Online Safety Policy/Guidance that may apply.
* Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
* The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
* They keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
* The use of the network/internet/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the head teacher/online safety coordinator for investigation/action/sanction.
* Monitoring software/systems are implemented and updated as agreed in school policies.

**Teaching and Support Staff**

All teachers and support staff should:

* Ensure that they keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
* Ensure that e-safety is taught at some point in the year.
* Be aware of the monitoring software/systems which are implemented and updated as part of the school’s policies.
* Have read, understood and signed the Staff Acceptable Use Policy.
* Report any suspected misuse or problem to the Head Teacher for investigation / action / sanction.
* Promote online safety issues in all aspects of the curriculum and other activities.
* Assist pupils in understanding and following the Online Safety Policy and acceptable use policies.
* Assist pupils in having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* Monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
* In lessons where internet use is pre-planned, assist pupils by guiding them to sites checked as suitable for their use.

**Designated Person**

The designated Person is the Head Teacher and DSL. They are aware of the potential for serious child protection/safeguarding issues that may arise from:

* Sharing of personal data.
* Access to illegal/inappropriate materials.
* Inappropriate on-line contact with adults/strangers.
* Potential or actual incidents of grooming.
* Cyber-bullying.

**Students/Pupils**

Students are responsible for using the school digital technology systems in accordance with the Student/Pupil Acceptable Use Agreement. They should:

* Have an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
* Be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
* Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school’s Online Safety Policy covers their actions out of school, if related to their membership of the school.

**Parents/Carers**

Parents/Carers play an important role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The school should take every opportunity to help parents understand these issues through newsletters, letters, website and information about national/local online safety campaigns/literature.

Parents and carers should also be encouraged to support the school in promoting good online safety practice and to be aware of the online safety policy and follow guidelines on the appropriate use of:

* Their own digital devices when on school premises or supporting school events and activities.
* Digital and video images taken at school events.
* Access to parents’ sections of the website and on-line student/pupil records.
* Their children’s personal devices in school.

**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.
* Issues such as cyberbullying and e-safety are built into the curriculum to encourage self –efficacy and resilience. Some children who have had previous experiences with internet bullying or with other additional needs may need additional support.

**Education of Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

* Key online safety messages should be reinforced as part of a planned programme of assemblies and class activities.
* Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
* Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
* Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
* Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
* Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
* In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

**Education of Parents**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

* Letters, newsletters, web site.
* High profile events / campaigns e.g. Safer Internet Day.
* Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ www.childnet.com/parents-and-carers.

**Managing Internet Access**

**Information Security System**

* The school ICT system security will be reviewed regularly.
* Virus protection will be updated regularly.
* Security strategies may be discussed with the Local Authority.

**E-mail and Online Communication**

* Staff may only use approved e-mail accounts on the school system.
* Staff to pupil communication must only take place via an approved education system or from within a learning platform and will be monitored.
* All incoming communication should be treated as suspicious and attachments not opened unless the author is known.
* The forwarding of chain letters is not permitted.

**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.
* The head teacher or their nominee 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
* Pupil’s full names will be avoided on the website and learning platforms including blogs, especially if associated with a photograph.
* Written permission will be obtained from parents and carers before any photographs are published on the school website. This is achieved through the photo consent form at the start of each academic year.
* Parents are clearly informed of the school policy on image taking and publishing.

**Managing Filtering**

* The school will work with the network manager to ensure systems to protect pupils are reviewed and improved.
* Any unsuitable on-line material should be reported to the head teacher.
* Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
* A log will be kept of any incidents related to children’s behaviour and inappropriate use of the internet. This will be used to identify patterns and behaviours and therefore inform policy and educational interventions.

**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.

**Protecting Personal Data**

* Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school will ensure that:

* It has a Data Protection Policy.
* It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
* Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
* The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented.
* Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
* It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
* Procedures must be in place to deal with the individual rights of the data subject.
* There are clear and understood data retention policies and routines for the deletion and disposal of data.
* Consideration has been given to the protection of personal data when accessed using any remote access solutions.
* All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
* All staff receive data handling awareness / data protection training and are made aware of their responsibilities.
* At all times it takes care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
* Personal data is used only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
* Data is transferred using encryption and securely password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

* The data must be encrypted and password protected.
* The device must be password protected.
* The device must offer approved virus and malware checking software.
* The data must be securely deleted from the device once it has been transferred or its use is complete.

**Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

* The official school email service may be regarded as safe and secure. Users should be aware that email communications can be monitored.
* Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
* Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
* Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**Social Media - Protecting Professional Identity**

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. The schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

* Ensuring that personal information is not published.
* Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
* Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff and parents should ensure that:

* Safeguarding children is paramount and is a key responsibility of all members of staff. It is essential that everyone at Willoughby School considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer must not communicate with children via social networking.
* No negative reference should be made in social media to pupils, parents / carers or school staff.
* They do not engage in online discussion on personal matters relating to members of the school community.
* Personal opinions should not be attributed to the school.
* Everyone within the Willoughby community has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.
* This policy relates to social networking outside work. Blogging and accessing social networking sites at work or at home using school equipment is not permitted, unless for professional purposes and authorised by the Head Teacher.

**Policy Decisions**

**Authorising Internet Access**

* All staff must read and sign the ‘employee code of conduct’ and ‘acceptable use policy’ before using any school ICT resource.
* The school will maintain a current record of all staff and pupils who are given access to school IT systems.
* Parents will be asked to sign and return a consent form.
* At Key stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials.

**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 in accordance with the school’s complaints procedures.
* Complaints of misuse by staff will be referred to the head teacher.
* Any complaints of a child protection nature must 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.

**Illegal Incidents**

**If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.**



**Other Incidents**

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

* Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).

Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

* Internal response or disciplinary procedures.
* Involvement by Local Authority or national/local organisation (as relevant).
* Police involvement and/or action.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

* Incidents of ‘grooming’ behaviour.
* The sending of obscene materials to a child.
* Adult material which potentially breaches the Obscene Publications Act.
* Criminally racist material.
* Promotion of terrorism or extremism.
* Other criminal conduct, activity or materials.

**Isolate the computer in question as best you can.**

**Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

**Communicating the Policy**

**Pupils**

* Appropriate elements of the e-safety policy will be shared with pupils, including teaching children not to speak with people online that they don’t know and being careful what they share about themselves (this is particularly relevant in preventing grooming and radicalisation).
* E-safety rules will be posted in all networked rooms.
* Pupils will be informed that network and internet use will be monitored.
* Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

**Staff**

* All staff will be given a copy of the e-safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
* Staff should be aware that the system is monitored and that professional standards are expected.
* All staff, through appropriate safeguarding training, will know how to respond if a child makes a disclosure.

**Parents**

* Parents will be notified of the policy in newsletters and the school website.
* The parents of all children at Willoughby Primary School will be asked to sign the parent/pupil agreement when they register their children.

Author: B. Smith

Date: Sept 2021

Review date: Set 2024

**Appendices**

* **Parents/carers consent form and e-safety rules**
* **Staff, governor and visitor acceptable use policy**
* **Use of digital images**
* **E-safety rules for KS1 and KS2**

**Parent/Carers consent form and e-safety rules**

All pupils will have access to the school’s computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

**Pupils Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Parent/Carer Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* As the parent or legal guardian of the above pupil, I have read and understood the attached school rules and now grant permission for my son/daughter to use the internet, school e-mail system, learning platform and other ICT facilities at School.
* I know that my son/daughter has signed an e-safety agreement and they have a copy of the school e-safety rules.
* We have discussed this document and they agree to follow the rules to support the safe and responsible use of ICT at School.
* I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.
* The school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and e-safety issues.
* I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child’s e-safety.

Parents Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Please complete and return to the school office.**

 **Staff, Governor and Visitor**

 **Acceptable Use Policy/ICT Code of Conduct**

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our working life in school. This policy is designed to ensure all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

* I appreciate that ICT includes a wide range of systems and devices including mobile phones, PDAs, digital cameras, email, social networking and may include personal ICT devices when used for school business.
* I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
* I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
* I understand that I am responsible for all activities carried out under my user name.
* I will only use the school email, internet, intranet, learning platform or any related technologies for professional purposes.
* I will ensure that personal data is kept secure and used appropriately, whether in school, taken out of school or used remotely when authorised by the head teacher or governing body.
* I will not install any hardware or software without permission.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* I will respect copyright and intellectual property rights.
* Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with consent of the parent, carer or staff member. Images will not be distributed outside the school network/learning platform without permission.
* I will ensure that my online activity both in school and outside school will not bring my professional role into disrepute.
* I will ensure that all electronic communications with parents, pupils and staff are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
* I will support the school’s e-safety policy and help pupils to be safe.
* I will report any incidents of concern regarding children’s safety to the e-safety coordinator, the Designated Person or their assistant.
* I understand that sanctions for disregarding any of the above will be in line with the school’s disciplinary procedures and serious infringements may be referred to the police.

**User Signature**

I agree to follow the code of conduct and support the safe use of ICT throughout the school

Full Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# E-safety Rules for Key Stage 1

|  |
| --- |
| **Think then Click** |
| We only use the internet when an adult is with us. | I only use the internet when an adult has given me permission. |  |
|  | I am kind on the internet and tell an adult if someone isn’t kind to me. |  |
|  | I will tell an adult if someone tries to talk or message me in an app or on the internet. |  |
|  | I can search within websites chosen by an adult. | We only use the internet when an adult is with us. |
| We only use the internet when an adult is with us. | I always ask an adult if I get lost on an app or website, or if something unexpected pops up. |  |
|  | I never tell anyone my name, age, school or where I live on the internet. |  |

**E-safety Rules for Key Stage 2**

|  |
| --- |
| **Think then Click** |
| * I will follow the SMART rules:
	+ I will stay SAFE by never give out my name, passwords or personal information online.
	+ I will never arrange to MEET anyone new that I have only chatted with on-line.
	+ I will not ACCEPT e-mails, or open pop-ups or messages, sent by someone I don’t know.
	+ I will question how RELIABLE information online is.
	+ If I’m not sure, or I see something that upsets me, I will TELL a responsible adult.
* We only use the internet when an adult is with us.I only use the internet if I have permission.
* I will only use websites or apps that an adult has chosen.
* I will use safe search engines for research.
* I will be polite and friendly when communicating with people online.
* I will seek permission from a responsible adult before posting an image or video of myself
 |

Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signed:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_