WAYFIELD PRIMARY SCHOOL

E-SAFETY POLICY

Reviewed: July 2018

Review Date: July 2019

This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Wayfield Primary School is committed to providing Quality First Teaching and a dyslexia friendly environment as a basic entitlement for all learners. As a school, we value the needs of all learners and foster a positive attitude towards pupils with dyslexia. We aim to teach all learners how to build on their strengths and minimise their weaknesses by bypassing their barriers to learning so that they are empowered to achieve to the best of their abilities.

Introduction

The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher.

There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.

- Describe how these fit into the wider context of our behaviour and PHSE policies.

- Demonstrate the methods used to protect the children from sites containing unsuitable material.

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 guardians.

At Wayfield, we feel that the best recipe for success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

Parents will be sent an explanatory letter and the rules, which form our Internet Access Agreement (Attached to the end of this document). This will form part of our welcome pack. We will also aim to disseminate any relevant published materials to parents.

Teaching and Learning

Why is Internet use important?

- We use the internet for a number of reasons:

- Internet use is part of the statutory curriculum and a necessary tool for learning.

- The Internet is a part of everyday life for education, business and social interaction.

- The school has a duty to provide students with quality Internet access as part of their learning experience.

- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online.

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;

- educational and cultural exchanges between pupils worldwide;

- vocational, social and leisure use in libraries, clubs and at home;

- access to experts in many fields for pupils and staff;

- professional development for staff through access to national developments, educational materials and effective curriculum practice;

- collaboration across networks of schools, support services and professional associations;

- improved access to technical support including remote management of networks and automatic system updates;

- exchange of curriculum and administration data with Local Authority and DFE;

- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.

- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- Because the quality of information received via radio, newspaper and telephone is variable and information received via the Internet, email or text message requires even better information handling and digital literacy skills.

- In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. Pupils should be made aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching and learning in every subject.

Managing Information Systems

How will information systems security be maintained?

- Virus protection will be updated regularly.

- Personal data sent over the Internet will be encrypted.

- Portable media may not used without specific permission followed by a virus check.

- Unapproved software will not be allowed in pupils' work areas or attached to email.

How will email be managed?

- Only school email addresses will be used for communication on the Wayfield iPads by children and teachers.
- Children will be permitted to contact each other using school email addresses for educational purposes only. Any breach of our accepted code will be dealt with in accordance with the Positive Behaviour Policy.
- Children will be taught how to block contacts, report unwanted behaviour on-line and turn off elements of the iPad that they do not wish to have enabled, for example alerts.
- Children will be taught to "Zip it, Block it, Flag it," in accordance with the UK Council for Child Internet Safety.
- Pupils may only use approved email or blogging accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal email accounts may be blocked.
- The forwarding of chain messages is not permitted.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

How will published content be managed?

- We have created a website that inspires pupils to publish work of a high standard.

- We use it to celebrate pupils' work, promote the school and publish resources for projects.

- Publication of information should be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate and editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.

- Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

- Images of a pupil will be published unless parents request otherwise. Pupils also need to be taught the reasons for caution in publishing personal information and images online (see section 2.3.6).

- Pupils' full names will not be used anywhere on the website in association with a photograph.

How will social networking, social media and personal publishing be managed?

- Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

- Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

- Although primary age pupils should not use Facebook, Instagram, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.

- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- Teachers cannot under any circumstances mention any references to their working lives on any social media.

- The school will control access to social media and social networking sites.

- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.

- Staff are advised not to run social network spaces for pupil use on a personal basis.

- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

How will filtering be managed?

- The school will work with KLZ to ensure that systems to protect pupils are reviewed and improved.

- If staff or pupils discover unsuitable sites, the URL must be reported to the ICT co-ordinator or a senior member of staff.

- The school's broadband access includes filtering appropriate to the age and maturity of pupils. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that staff believe is illegal must be reported to the Head teacher who will inform the appropriate agencies.

- We keep up to date with new technologies, including those relating to mobile phones and handheld devices, and be ready to develop appropriate strategies.

- There are dangers for staff however if personal phones are used to contact pupils or families and therefore this will only be done when authorized by a senior member of staff.

- Abusive messages should be dealt with under the school's behaviour and anti-bullying policy.

- Emerging technologies will be examined for educational benefit and the Head teacher in consultation with staff will give permission for appropriate use.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.

- Pupils are not allowed to bring mobile phones into school. Under certain circumstances exceptions can be discussed with the Head teacher, so that pupil mobile phones can be kept in the school office. Parents must complete the permission slip to acknowledge that the school takes no responsibility for phones which are left in the office.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The General Data Protection Regulation (2018) ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly.

It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The General Data Protection Regulation (2018) applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

- The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

- The eight principles are that personal data must be:

  - Processed fairly and lawfully
  - Processed for specified purposes
  - Adequate, relevant and not excessive
  - Accurate and up-to-date
  - Held no longer than is necessary
  - Processed in line with individual's rights
  - Kept secure
  - Transferred only to other countries with suitable security measures.
  - This section is a reminder that all data from which people can be identified is protected.
  - Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

Policy Decisions
How will Internet access be authorised?

- We allocate Internet access for staff and pupils on the basis of educational need. It should be clear who has Internet access and who has not.
- Authorisation is as individuals and usage is fully supervised. Normally all pupils will be granted Internet access.
- Parental permission is required for Internet access in all cases as new pupils join Wayfield.
- All staff must read and sign the Code of Conduct before using any school ICT resource.

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return consent form for pupil access. Parents will be informed that pupils will be provided with supervised Internet access.

How will risks be assessed?

- Wayfield will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Medway LA can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly and after every breech of this policy.

How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Head of School. If the complaint is about the Head of School this should be reported to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaints procedure. Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

How is the Internet used across the community?

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety though regular information sent home with children and through advice on our website.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- We also hold an E-safety evening for parents yearly. This is for parents of children from Nursery to Year 6.

How will Cyberbullying be managed?

- Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.
- It is essential that pupils, Wayfield staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse.
- Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying:

  http://www.digizen.org/cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify bullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Sanctions for those involved in Cyberbullying may include: The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers will be informed and the Police will be contacted if a criminal offence is suspected.

Other E-safety Issues

Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the world wide web.

Pornography – many children will come across some type of pornographic content when searching the Internet. Children are taught about what to do if they come across this type of material and who to speak to.

How will iPads and learning environments be managed?

- SLT and staff will monitor the usage of the iPads by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.

- Pupils/staff will be advised on acceptable conduct and use when using the iPads. Only members of the current pupil, parent/carers and staff community will have access to the IPads.
- All users will use technology respectfully. They will respect the rules of consent and permission and will only upload appropriate content onto the iPads.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled.

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.

c) Access to the iPads for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A pupil's parent/carer may be informed.

Communication Policy

How will the policy be introduced to pupils?

- At Wayfield we teach about e–Safety as a computing lesson activity and as part of every subject whenever pupils are using the internet.

- Pupil instruction in responsible and safe use should precede Internet access every time they go online.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

We will use the following e–Safety programmes:

Think U Know: www.thinkuknow.co.uk
Childnet: www.childnet.com
Kidsmart: www.kidsmart.org.uk
Safe Social Networking: www.safesocialnetworking.com

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff and published on the school website.
- To protect all staff and pupils, the school will implement Acceptable Use Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user; discretion and professional conduct is essential.

- Staff training in safe and responsible Internet use both professionally and personally will be provided, both internally and externally.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.
- Parents will be requested to sign an e–Safety/internet agreement as part of the school's on entry procedures. Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Policy Management

This policy is linked to the following mandatory school/centre policies: Child Protection, Whistle Blowing, Health and Safety and Home School Agreements**.**

Who will review the policy?

The e–Safety Policy and its implementation will be reviewed annually

Signed:…….…….. T Williams, Head Teacher

Date:……

Signed:…….. R McDonald, Chair of Governors

Date:……

Appendix 1:Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (Which is currently: Staffmail)
- I will only use the approved school email, school MLE or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti- virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.

- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title
.....

School
.....

Authorised Signature (Head Teacher)

I approve this user to be set-up.
Signature ..... Date.....
Full Name ..... (printed)

Appendix 2: Internet Agreement

All pupils and their parents / guardians will be asked to read and sign an agreement covering the expectations we have of pupils using the Internet in school.

Wayfield School Pupil Internet Agreement

Acceptable Use Policy (AUP)

This is to be read through with your parent(s) and then signed. You will be allowed Internet Access after this is returned to school.

At Wayfield, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher. Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.

Pupils must ask permission before accessing the Internet.
Pupils should not access other people's files unless permission has been given.
Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
No program files may be downloaded to the computer from the Internet. No programs on disc or CD Rom should be brought in from home for use in school.
Personal printing is not allowed on our network for cost reasons (e.g. pictures of pop groups/cartoon characters).
No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

I have read through this agreement with my child and agree to these safety

Signed: _____ (Parent/Responsible Adult)
Name of child: _____

Appendix 3 : Please read Home School iPad Agreement