Woodside Group
E-Safety Policy

1. Who will write and review the policy?

Our e-safety Policy has been written by the E-Safety Coordinator in conjunction with the school DSL. The policy has been agreed by the SLT and it will be reviewed at least once a year. Changes will be made immediately if technological or other developments so require.

2. What is E-Safety?

• E-Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets, laptops, game consoles. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.
• This policy will operate in conjunction with other school policies including those for ICT, Behaviour, Bullying, PSHE and Safeguarding & Child Protection.
• 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.
• Internet use is a part of the statutory curriculum and a necessary tool for learning.
• Internet access is an entitlement for students who show a responsible and mature approach to its use.
• The Internet is an essential element in 21st Century 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.
The school has a Designated E-Safety/ICT Coordinator (Michael Sherwood) who works closely with the school Designated Safeguarding Lead (Dan Long) to ensure that the school fulfills its E-Safety responsibilities. They work in

collaboration with the Head of PSHE in order to ensure this policy meets the ever-changing issues relating to the Internet and its safe use. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

3. How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Cultural, 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 support services, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including email.

4. How can Internet use enhance learning?

- The school Internet access will be designed expressly for school use and will include filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Staff will choose appropriate material to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line 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.

5. How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the E-Safety Officer. Pupils must follow the procedure for reporting unsuitable Internet content which is shared with all pupils by their teacher.

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

MANAGING INFORMATION SERVICES

6. How will our ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Use of data storage facilities by pupils within school is prohibited to protect against virus transfer.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The E-Safety Officer will ensure that the system has the capacity to take increased traffic caused by Internet use.

7. How should the school website content be managed?

- The point of contact on the website will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school. At present editorial responsibility for all other areas of the website is the responsibility of Jonathan Lakin.
- The Website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Can pupils' images or work be published?

- Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be identifiable.

- Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.
- Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.

9. How will social networking and personal publishing be managed?

- 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 e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should 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 eg. house number, street name or school.
- Students should be advised not to publish specific and detailed private thoughts.

10. How will filtering be managed?

- The school will work in partnership with parents and the Local Authority to ensure systems to protect pupils are reviewed and updated.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the E- safety officer.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate.

11. How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The sending of abusive or inappropriate messages/communication is forbidden. See 'Student Mobile Phone Policy' for further information.

POLICY DECISIONS

12. How will Internet access be authorized?

- All staff and pupils will initially be granted Internet access.

- Parents will be informed that pupils will be provided with supervised Internet access.
- Pupils will not be allowed to use computers with Internet unless they are directly supervised by a member of staff during lesson time.
- Guidelines relating to Internet safety are visible from all machines with Internet access, throughout the school.

13. How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot 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.
- The school should monitor wireless, infra-red and Bluetooth communication.
- Methods to identify, assess and minimize risks will be reviewed regularly.
- Use of mobile phones is not permitted during lessons unless express permission is given by a member of staff.
- The E-Safety Officer will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.
- The school has a mobile phone/MMD policy.

14. How should personal data be protected?

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

15. How will E-safety complaints be handled?

- Responsibility for handling incidents will be delegated to the E-Safety Officer.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

• As with other serious issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
Sanctions available include:- interview/counselling by senior member of staff/class teacher/teaching assistants; - informing parents or carers ; - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

COMMUNICATIONS POLICY

16. How will the policy be introduced to pupils?

• Pupils will be regularly informed that Internet use will be monitored.
• Instruction in responsible and safe use should precede Internet access.

17. How will the policy be discussed with staff?

• Staff should be aware that Internet traffic can and will be monitored. Discretion and professional conduct is essential.
• The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Senior Leadership Team.
• Staff training in safe and responsible Internet use, and on the school E-Safety Policy will be provided as required.
• The school will liaise with local organisations such as Leicestershire County Council to establish a common approach to E-safety
• The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
• All staff will be given the School E-Safety Policy and its application and its importance explained

18. How will parents' support be enlisted?

• Parents' attention will be drawn to the School E-Safety Policy in newsletters, at Parent Support Groups and on the school website.
• Internet issues will be handled sensitively to inform parents without undue alarm.
Parents will be sent home a school internet safety leaflet to sign, which will ensure they have read and understood possible E-safety issues within a school/s.