INTERNET SAFETY POLICY

This policy applies to ALL members of staff.

This aim of this policy is to protect:

- all school IT equipment whether used on or off the school premises
- the integrity of all school data whether accessed on or off the school premises.
- the confidentiality of school data whether accessed on or off school premises.

To comply with Data Protection laws.

- Our E-Safety and IT Acceptable use Policy (AUP) has been written by the school, taking into consideration Local Authority and Government guidance. It has been agreed by the Senior Leadership Team and approved by Governors. It will be reviewed annually.
- Use of the school's IT equipment by any members of the school community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the school Governing Body.

1. Why the Internet and Digital Communications are important

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

2. Internet use will enhance and extend learning

- The school Internet access will be designed expressly for student use and will include filtering appropriate to the age of students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

3. Pupils will be taught how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4. Information system security

- School IT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

5. Use of school equipment.

- All school IT equipment must be used appropriately at all times with regard to e-safety, health and safety and rules of confidentially to maintain professional standards on and off the school site.
- All school IT equipment and school software may only be used by members of staff whether on or off the school site.

6. Management of School E-Mail

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.

7. Management of School Website Content

- The contact details given online will be the school address, school e-mail and telephone number. Staff or student personal contact information will not be published, except within the secure Learning Portal where student contact details will be available to staff users only.

8. Publishing students' images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Website.

9. Social networking, chat rooms and personal publishing

- The school will control access to social networking sites, and consider how to educate students in their safe use.
- Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Students **AND STAFF** will not be allowed access to **public** chat rooms using the school's network or portable IT equipment provided by the school whether accessed on or off the school site.

10. Managing filtering

- Access to the Internet is provided to the school by the Local Authority. The school will work in partnership with the Local Authority to ensure that systems to protect pupils are reviewed and improved regularly.
- If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator and the Headteacher.

11. Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the Students' age.

12. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- **MOBILE PHONES WILL NOT BE USED** without permission during lessons or formal school time by students or staff.

13. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

14. Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for IT' before using any school IT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- Parents will be informed that students will be provided with supervised Internet access.
- Parents and pupils will be asked to sign and return a consent form.
- Students must apply for Internet access individually by agreeing to abide by the Responsible Internet Use statement.

15. Assessing Risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

16. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.

17. Informing students about the E-Safety and Acceptable Use Policy

- E-Safety rules will be posted in all rooms where computers are used.
- Students will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.

18. Staff and the E-Safety and Acceptable Use Policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor IT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with pupils or their parents can lead to misunderstandings or even malicious accusations. **All Staff must take care always to maintain a professional relationship.**

19. Enlisting Parental Support.

- Parents' attention will be drawn to the School Internet Policy in the school prospectus.

20. Community use of the Internet

- Adult users will need to sign the acceptable use policy.
- Parents/carers of children are required to sign an acceptable use policy.

Staff Code of Conduct for IT

To ensure that members of staff are fully aware of their professional responsibilities when using any school IT equipment, information systems and when communicating with pupils on or off school premises, they are asked to sign this code of conduct. Members of staff should consult the school's E-Safety and Internet Acceptable Use Policy for further information and clarification.

- I understand that it is a criminal offence to use the school IT system or school IT equipment both on and off the school site for a purpose not permitted by its owner.
- I appreciate that the school IT includes a wide range of systems and equipment, including mobile phones, laptops, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business on and off school site.
- I understand that school information systems may **not** be used for private purposes without specific permission from the Headteacher.
- I understand that portable IT equipment and school software can only be used by members of staff.
- I understand that my use of school IT equipment, information systems, Internet and email may be monitored and recorded to ensure policy compliance whether used on or off the school premises.
- I will respect the security of the system and data and maintain confidentiality. I will not disclose any password or security information to anyone other than an authorised system manager
- I will not install any software or hardware without permission on any school equipment whether on or off school premises.
- I will not permit non members of staff to install or use any software or hardware without permission on any school equipment whether on or off school premises.
- No personal equipment, including cameras, mobile phones, laptops or tablets will be used to take or store photographs or videos of pupils.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the Designated Child Protection Coordinator or Headteacher.
- I will ensure that all electronic communications with pupils, including e-mail and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may

be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for IT.

Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	
Signed: _____ _____	***Date:*** _____
Print name: _____	