THE BISHOPSWOOD SCHOOLS FEDERATION

E-Safety Policy

Introduction

The ICT resources used by pupils in Bishopswood Schools Federation 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 that are 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 Bishopswood Schools Federation, 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.

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.

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.

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 be 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 published content be managed?

- We use it to celebrate pupils' achievements, 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 Executive 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.
- 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.
- 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.
- 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 to think before 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.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- 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 Hampshire IT and Agile ICT 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 Computing 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 Executive Head teacher or a senior member of staff who will inform the appropriate agencies.
- We keep up to date with new technologies, including those relating to mobile phones and handheld devices, and are 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 Executive 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. Please refer to our Mobile Phone Policy for details.

How should personal data be protected?
Please refer to our Date Protection Policy for details.

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.
- 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 informed that pupils will be provided with supervised internet access.

How will risks be assessed?
- Bishopswood Schools Federation 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 Hampshire 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 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 regular E-safety meetings for parents. These are for parents of children from EYFS to Year 6.

How will Cyberbullying be managed?
- Cyberbullying is bullying that takes place using technology, e.g. via mobile phone or online (for example email, social networks and instant messenger)

- Staff at Bishopswood Schools Federation 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. DFE 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 (please read alongside our Child Protection and Safeguarding Policies)
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.

Communication of Policy

How will the policy be introduced to pupils?
- At Bishopswood 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.

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 also implement an Acceptable Use of ICT 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 as part of Safeguarding training.

How will parents' support be enlisted?
- Parents' attention will be drawn to the School e–Safety Policy 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.
- 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 policies: Child Protection, Safeguarding, Whistle Blowing, Health and Safety, Anti-Bullying, Home School Agreements, Teaching & Learning, GDPR, Staff Acceptable use of ICT

Who will review the policy?
The e–Safety Policy and its implementation will be reviewed annually by the Governing Body.

Policy Reviewed – November 2021

Next Review – November 2023