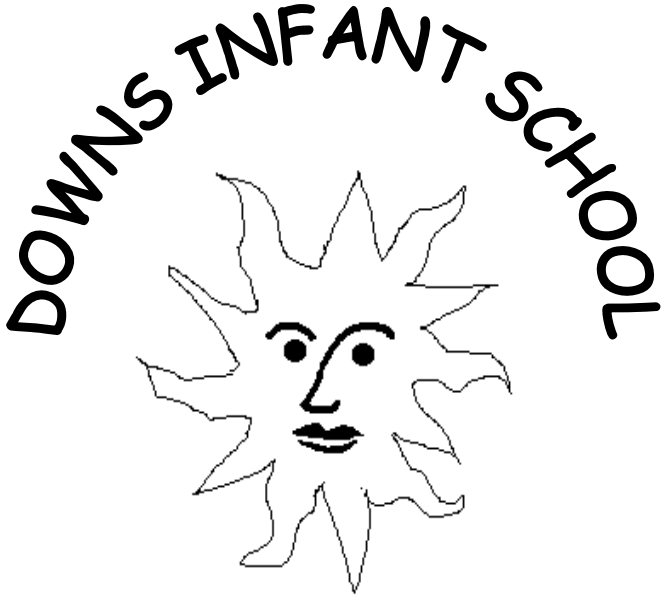


# E-safety Policy
# Ratified : June 2015
# Review Date : June 2018

**Computing Coordinator – Anna Korman**

**Contents**


1. Emerging Technologies.
2. Why is internet use important in school?
3. How does the internet benefit education?
4. Using the internet to enhance learning at Downs Infant School.
5. Pupils will be taught.
6. Before using the internet as a teaching tool, Staff should:
7. Social Media.
8. How will e-mail be managed ensuring safety for pupils?
9. How should the School Website content be managed?
10. Photographic, video and audio technology.
11. How will internet access be authorised?
12. How will the risks be assessed?
13. How will filtering be managed?
14. How will the policy be introduced to pupils?
15. How will staff be consulted and made aware of this policy?
16. How will ICT system security be maintained?
17. How will complaints regarding internet use be handled?
18. How will parents' support be enlisted?
19. Staff Use.

This Policy should be read in conjunction with our Computing, Child Protection and Behaviour Policies.

**1. Emerging Technologies:**
The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media, but the principles set out in this policy must be followed irrespective of how the medium develops.

Many emerging technologies offer the potential to develop new teaching and learning tools. Mobile communications, wide internet access and multimedia present opportunities which need to be evaluated to assess risks, to establish benefits and to develop good practice. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

**2. Why is internet use important in school?**
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 information (SIMS) and business administration systems.

The internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.

Internet use is a part of the statutory National Curriculum for Computing (DfE, September 2015 requiring pupils to learn how to communicate safely and respectfully online, keeping personal information private and to recognise common uses of information technology beyond the school.

Children may 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?**
All internet access should ***enrich and extend learning activities.*** Access should reflect the curriculum requirements and age of pupils. 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.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks.
- Exchange of curriculum and administration data with the LA and DfE.

- Peer support for children and staff.

**4. Using the internet to enhance learning at Downs Infant School:**

- Staff will guide pupils to 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.
- A member of staff will always be supervising in the area when the internet is used **- aimless surfing should never be allowed.** It is good practice to teach pupils to use the internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question "Why are we using the internet?"
- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Class email addresses will be used if required - never personal pupil emails.

**5. Pupils will be taught:**

- What internet use is acceptable and what is not and given clear objectives for internet use.
- The effective use of the internet in research, including the skills of knowledge, location and retrieval.
- How to use search engines such as Google sensibly using appropriate search words.
- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- To understand why you should acknowledge the source of information used and to respect copyright.
- About password security.
- E-safety rules.
- About cyberbullying (See Safeguarding and Behaviour Policies).

**6. Before using the internet as a teaching tool, Staff should**:

- Ensure that the use of internet derived materials by pupils complies with copyright law and that all websites reflect gender and cultural diversity and are age appropriate to our children.
- Staff must view websites and content before use with children.

**7. Social Media:**

Staff members need to be aware that everything they post online is public, even with the strictest privacy settings. Once something is online, it can be copied and redistributed and it is easy to lose control of it. They should therefore assume that everything they post online will be permanent and can be shared.

Staff must be conscious at all times of the need to keep their personal and professional online lives separate.

- Staff are expected to exercise extreme caution over their personal use of social networking sites such as *Facebook* and *Twitter* at home, restricting access, settings and controlling content to ensure that all school matters remain confidential and that they present a professional persona.
- When publishing material to websites and elsewhere, staff and pupils should consider the thoughts and feelings of those who might view the material. Material that victimises or bullies someone else, or is otherwise offensive, is unacceptable.
- Pupils will not be allowed to access inappropriate age related sites, chat rooms, forums newsgroups or social networking sites e.g. *Facebook, Twitter.*
- Any form of bullying or harassment is strictly forbidden.
- A dynamic risk assessment is carried out before pupils are allowed to use a new technology in school. (Please see Social Networking Policy)

**8. How will e-mail be managed ensuring safety for pupils?**

- Whole-class e-mail addresses should be used at Key Stage 1 and below.
- Pupils may only use approved class e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication or via a personal web space, such as address or telephone number, or arrange to meet anyone.
- Personal email or messaging between staff and pupils should not take place.
- Access in school to external personal e-mail accounts may be blocked by our school's filtering system.

**9. How should the School Website content be managed?**

The school website enables pupils to access internet based resources used in the class at home with their parents/ carers. This encourages pupils to continue to develop their knowledge in a certain subject area and build on skills in English and Maths.

- Photographs published on the website that include pupils are selected carefully and do not enable individual pupils to be clearly identified.
- Pupils' full names are not used anywhere on the school website particularly in association with photographs.
- The Head teacher or nominee takes overall editorial responsibility and ensures that content is accurate and appropriate.
- The website complies with the Ofsted and 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 it has been obtained.

**10. Photographic, video and audio technology:**

These technologies fall under the Data Protection Act. Storage, copying and publication (i.e. e-mailing to someone, etc) must only be done securely and for the use it was intended for. Special consideration needs to be given to mobile devices such as memory sticks/ cards, tablets, laptops and cameras.

- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Parents accompanying school trips may not take pictures of children other than their own on cameras and mobile phones. These pictures are for their personal use only and not to be shared anywhere including social media.
- Staff must not take pictures or videos of children using their own devices.
- Staff may use photographic or video devices (Including digital cameras and iPads) to support school trips and curriculum activities (See Acceptable Use for iPads policy).
- The school only has access to sites which have passed through the LA filter/ web washer and seen to be safe to use in school.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken and be risk assessed for suitability before use.

**11. How will internet access be authorised?**

- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents are hereby informed that pupils will be provided with supervised internet access.
- Pupils are not issued individual email accounts, but will be authorised to use a group/class email address under supervision.

**12. 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. 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 are reviewed regularly.
- The head teacher ensures that the e-Safety policy is implemented and compliance with the policy monitored.
- Access is blocked and strictly forbidden to any websites that involve gambling, or financial scams.

**13. How will filtering be managed?**

Downs Infant School's internet filtering is supplied by Brighton & Hove City Council. It is maintained by BHCC School ICT & Traded Services but the school has a level of control over the sites that are available to pupils. Authorised staff also have access to resources such as YouTube and Google Images.

- Staff have to attend training and sign an acceptable use policy to gain this access.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet Service Provider via the Computing Coordinator.
- Any material that the school believes is illegal must be referred to the BHCC School ICT & Traded Services helpdesk and the police.

**14. How will the policy be introduced to pupils?**

- Pupils are informed that internet use will be monitored.
- Instruction in responsible and safe use should precede internet access.
- Responsible internet use is included in Computing teaching across the EYFS and KS1 curriculum covering both school and home use.

**15. How will staff be consulted and made aware of this policy?**

- All new staff are taken through the key parts of this policy as part of their induction.
- All staff including teachers, supply staff, classroom assistants and support staff, are provided with the School e-Safety Policy, and have its importance explained by the Computing Co-ordinator.
- Staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Breaching this e-safety policy may result in disciplinary action being taken.

**16. How will ICT system security be maintained?**

- It will be the responsibility of BHCC and the IT Technician along with the Head teacher and Computing Coordinator to ensure that the IT system security is maintained.
- Security strategies will be discussed with the Schools' IT Support team regularly.
- The school's server will be backed up to an offsite location each night.
- Anti-Virus protection will be updated regularly.
- The school's wireless internet is secure and password protected.
- The security of individual staff and pupil accounts will be reviewed regularly.
- The administrator account password will be changed if it becomes known.
- Computers (including mobile devices) may not be connected to the school network both physically or wirelessly without specific permission.

- Software will not be installed/removed from computers without specific permission.
- Security of any new cloud-based data storage will be checked thoroughly to ensure it complies with B&H requirements (e.g. Incerts).
- The Computing coordinator / network manager will review system capacity regularly.
- Disposal of old IT equipment complies with requirements of the Data Protection Act.
- All teaching staff are provided with a password protected safe stick to transfer school documentation on as is the head teacher and bursar. This is to ensure confidentiality and data protection of school information, including data which is able to identify an individual.
- All school related communication must be done using a school approved email account.

**17. How will complaints regarding internet use be handled?**

- Responsibility for handling incidents will be delegated to the head teacher.
- Any complaint about staff misuse must be referred to the Head teacher.
- There is a formal complaints procedure in place.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions available include:

- Interview/counselling by Head teacher;
- Informing parents or carers;
- Removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including the website.
- (See Behaviour Policy)

**18. How will parents' support be enlisted?**

- Parents' attention will be drawn to the School E-safety Policy in newsletters, the school prospectus and on the school website.
- Internet issues are handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet are made available to parents on the Website.
- Interested parents will be referred to organisations such as Thinkuknow, Parents Online (web addresses for e-safety support sites attached) through school newsletters and on the website.

**19. Staff Use**

- Staff users will need to sign the e-safety policy or alternatively an acceptable use policy.

- Staff are encouraged to use ICT responsibly for professional purposes. Staff are able to make limited private use of school ICT equipment, but only outside their working hours.
- Staff are not permitted to attempt to access unsuitable sites using school equipment or on school premises.
- Even when using personal equipment professional standards of conduct need to be maintained and breach of this is likely to lead to disciplinary action.

- **Portable media**- Under data protection staff need to ensure the secure storage and limited access to any data which can identify any individuals. This includes photographs and other data on cameras, mobile phones, iPads, laptops, memory sticks and cards, CD's, etc. keeping media in the car boot while parked, cameras with memory cards used by family members, theft of media from the home address and loss of memory sticks would be examples of undesirable events which would breach the Data Protection Act.

- **Mobile phones**- Staff should not use their mobile phones during 'contact hours' unless agreed by the Head teacher.
- Children should not bring mobile phones in to school.

- **E-mail accounts** - All staff are issued with a school hosted e-mail account which should be used for professional purposes. Private e-mail accounts should not be used for work related business.