



## Highworth Combined School & Nursery

### E-safety Policy

This policy was written/updated by: Megan Holloway

This policy was reviewed by the Curriculum Committee

This policy was adopted/ratified on: \_\_\_\_\_

This policy is to be reviewed by: Summer 2020

## Highworth Combined School

# E-safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of the school. Highworth Combined School recognises that the internet and other digital technologies provide a vast opportunity for children and young people to learn. Unlike any other mode of technology, the internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning. As part of our commitment to learning and achievement we want to ensure that the internet and other digital technologies are used to:

- Raise educational standards and promote pupil achievement
- Develop the curriculum and make learning exciting and purposeful
- Enable pupils to gain access to a wide span of knowledge in a way that ensures their safety and security.

To enable this to happen we have taken a whole school approach to e-safety which includes the development of policies and practices, the education and training of staff and pupils and the effective use of the School's infrastructure and technologies. We are committed to ensuring that **all** our pupils will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding them.

### Pupils

Whilst the use of new technology is very important, it must be balanced with educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned e-safety curriculum is provided as part of Computing/PSHCE and is regularly revisited
- Key e-safety messages are reinforced as part of assemblies and class based activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the Internet Agreement and encouraged to adopt safe and responsible use both within and outside school. Pupils are expected to sign the Internet Agreement at the start of each school year
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs,)
- Pupils may only use approved e-mail accounts on the school system
- Information is permanently displayed in the school corridor advising pupils about how to keep themselves safe online
- NSPCC visit annually to run assemblies and workshops to provide children with information and guidance
- Pupils must not reveal personal details of themselves or others in e-mail communication.

## **Staff**

- All staff must sign the Confidentiality Agreement at the start of each year and a copy is kept on file
- Any information downloaded must be respectful of copyright, property rights and privacy
- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to internet access, data protection and use of software, both in and out of school.

## **Parents/carers**

All parents sign a Home School Agreement at the start of each year which includes the Internet Agreement. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore provide information and awareness to parents and carers through:

- Letters and newsletters
- Useful e-safety links on the school website
- Parents/Carers information workshops
- High profile events/campaigns e.g. Safer Internet Day
- Information through the NSPCC's 'Share Aware' resources

## **Technical – infrastructure/equipment, filtering and monitoring**

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provided by Bucks County Council. Content lists are regularly updated and internet use is logged and regularly monitored.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might

threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software

- The use of removable media is now restricted in light of new GDPR regulations.

### **Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, images of children other than their own should not be published/made publicly available on social networking sites
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- All staff are made aware of which children are/are not permitted to be photographed and this is adhered to at all times
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless parental permission has been sought beforehand.

### **Reporting e-safety concerns**

If any member of staff has a concern about the safety of a child, they will follow the same procedures as a safeguarding concern by filling in a safeguarding slip on Behaviour Watch. The DSL (or additional DSLs) will follow this concern up promptly.

### **Equal Opportunities**

Highworth acknowledges its legal duty to make reasonable adjustments for disabled children and children with special educational needs (SEND). This policy has been written in accordance with and meets the requirements of the Equality Act 2010.