E Safety Policy 2017

Aim

The aim of this policy is to ensure the safety of all HBN ICT users.
To ensure that all parties - children, staff, and parents are clear on the relevant routines, policies and procedures.

Staff responsibilities

Teaching staff have a vital and very responsible role to play in the safe use of ICT equipment within the school community. If a member of staff has any doubts with regard to a particular issue then please speak to the Headteacher, Mrs Sutton or Miss Johnston.
All Teachers and Support Staff must ensure that this policy is understood and followed by all children.
The word 'teacher' in this policy should be taken to include support staff and other adults working with the children at the direction of the Class Teacher.
It is essential that all teaching staff:-

- Model good practice
- Adhere to all relevant policies including the AUP, behaviour policy, anti bullying policy and safeguarding policy
- Embed e-safety across the curriculum by taking every opportunity when equipment is in use to reinforce positive behaviours.
- Know how and when to escalate e-safety issues
- Maintain a professional level of conduct in their personal use of technology both within and outside school.
- Take personal responsibility for their professional development in this area and acknowledge that it is an essential resource and skill, that they must all use and they must enable the children to facilitate.
- Ensure that provision for vulnerable students is educationally appropriate.

Keeping everyone safe

Electronic equipment has to be used safely and sensibly. The use of the internet or any electronic device for bullying, harassment, sexual exploitation, racial or hate motivated incidents will result in appropriate consequences (see behaviour and anti bullying policy and disruption to learning protocol).

Devices

With reference specifically to all handheld devices (including mobile phones) :-

- Memory sticks belonging to a child must not be used in a school device. Files that need to be transfered between home and school should be done so via the pupils Google Drive or the cloud.
- Mobile phones - It is understood that some parents particularly of children traveling home alone may prefer the child to bring a phone to school. In school such a phone must be turned off and is the child's own responsibility. All mobiles must be left in the school office for the duration of the school day.
- ipads / ipods - These items are too valuable and should not to come into school.
- Digital cameras - Digital cameras from home are not necessary. School cameras will be used if necessary for work in school or for trips.
- Laptops - If required, they will be provided by school.
- Kindles / E reader - These items are too valuable to come into school. If required they will be provided by school.

Exceptions to these rules may be made at the discretion of the class teacher after consultation with the Headteacher on the last day of term. Any device should not be connected to the school WI-FI network.
Accidental or/and Deliberate access - In order to avoid deliberate access to unsuitable material through the internet no child is allowed access to a computer when a member of the teaching staff is not present.
All teaching staff have been shown how to view all the open windows on children's laptops in use at any one time. All teaching staff must only have a group of children working on the internet at any one time that they feel they can adequately oversee. Members of staff supervising children on the internet must regularly check that they do not have multiple tabs open, or windows mimimised to the dock and should check children's history to see what sites they have been accessing.
If a child does access some material regarded as unsuitable then the teacher concerned must inform the

Headteacher immediatly, and after advice inform parents.

Illegal Access

The definitive of "inappropriate" material can only be made by age and with an understanding of individual families circumstances.

However, in school the loc parentis decision has to be made by a member of the teaching staff. Therefore the "strict" settings of the DEC are to be used as guidance.

Attention has to be taken of the language used, blood and gore, and sexually explicit material. Access to You Tube, and other multi media sites is not acceptable in school by pupils.

As a school we will only use films with a rating that is approved legally for the correct age range i.e. 'U' and 'PG' (with the parents permission) ratings only for dvd / videos.

Care should be taken when using pictures from the internet that copyright laws are not broken. If in doubt then you should contact the owner or administrator of the site and ask for permission to use an image. A copy of their reply must be kept.

Access to the internet

Access to the internet should always be under the direct supervision of a teacher. Direct supervision involves working in the same teaching space as a member of the teaching staff to enable regular observation of the web sites visited by children.

If required the ICT co ordinator will be asked to check the history of sites that a child has visited. A member of the teaching team must ensure that they feel able to monitor and supervise the whole group working on the internet at any one time or reduce the number of pupils to a number that they are more comfortable with.

Children must not use the internet at lunch times or break times.

The school internet must not be used to carry out any illegal activities e.g. downloading music, videos or photographs. DEC equipment must not be used to share files if you do not own the copyright.

Web filtering

The web feed in school is filtered. However, it is not infallible.

All teaching staff should ensure that children searching Google Images do so with 'Strict filtering' enabled.

If there is a particular website that is blocked that you feel would be of benefit to the education of the children, then you should e-mail the help desk to request it be unblocked. (Ensure that you send them the correct url.) The Head Teacher (HT) should be copied into this e-mail.

Use of 3G to bypass web filtering

3G technology should not be used to bypass the web filter for any website that you wish pupils to view. If you wish to view a blocked website outside of teaching time for your own personal use then it must not be one which could bring the school or DEC into disrepute.

Use of Web 2.0 (wikis, blogs)

All pupils and staff must only post comments on wikis, blogs or forums using their own user ID and password.

Comments must not enable individuals in images/ photos to be identified.

Comments by staff on any website, wiki or forum that could bring the school into disrepute will lead to disciplinary proceedings.

Pupils must also learn to need for responsibility and respect when expressing their views on an internet 'forum'.

Social networking sites

The use of social networking sites by children is not allowed within school. Social networking sites include Facebook, Twitter, Myspace, Beebo, Club Penguin imbee, tweenland and Moshi Monsters. If you are unsure if a website is a social networking site speak to the HT. Access to these sites can be arranged for educational reasons. If you need / want to access speak to the HT. (A detailed lesson plan is a pre requisite to any arrangements being made.)

As a school we are ethically obliged to make parents and children aware of the legal lower age limit for access to these sites.

We will with support begin to teach children how to remain safe online, including understanding the use and dangers of Social Networking Sites and specifically cyber bullying. (See ICT curriculum document)

Personal Data

School's storage and use of images

It is Very important to note and remember that all images legally remain the property of the person or

person's in the photograph or image. They should not be posted on a DEC website / wiki without the written permission of the child's legal parent of guardian or the person themselves if over 18.
Each child will have a permission slip completed by a parent or guardian at the beginning of every school year. A list of children whose photographs should not be published is held in the School Office.
Images may only be posted - un named on the school wiki. If this is not possible then only first names should be used. Great care must be taken that information on the site does not give away the individuals name or other personal information.
If you wish to upload pictures of children to any website not run by the DEC (with the exception of IOM Newspapers) written permission should be obtained from the childs parents. This written permission should be kept in the child's file in the school office.
All images of all children must be deleted from the school website, server and individual laptops as soon as is practically possible after each child leaves the school.
Images must only be taken using a school owned camera. Teachers must not use their own mobile phone to take photographs of children.
Parent helpers on school trips should not take photos of children other than their own, using their own camera.
All images must be downloaded from school cameras and then deleted off the camera's memory as soon as is practical after the trip but must be done within 24hrs.
Sensitive Data
The school holds a large amount of sensitive date. This includes attendance and admission data, SEN records and reports, CAF/ Child Protection information, children's assessment data, members of staff's contact details, personal information, PM documents and job descriptions. Access to all these files will also be subject to the Information Sharing Policy and requirements.
Monitoring of the use made by students and supply teaching staff of children and staff personal information will include a confidentiality discussion and if access is enabled to laptops then a check will be run to ensure appropriate material is deleted and that inappropriate access does not occur. Therefore the use of electronic equipment must be done so in a secure manner. It must be kept on an encrypted hard drive with a 'secure' password.
Sensitive data must not be stored on any removable media e.g. pen drives, Cd's, DVD's etc. regardless of wether it is encrypted or not.

If you believe that you may have lost sensitive data, then you should inform the HT straight away. If this is not possible then you should inform the Department of Education's ICT team (686081). This must be done as soon as possible and within 12hrs.
Passwords
All staff must ensure that all passwords used are secure. As a minimum they should be 8 characters, and contain a mixture of upper and lower case letters, numbers and symbols. Generic or easily guessable passwords e.g. changeme, 1234, fred, qwerty, password, iloveyou, your user id, or names of pets or family members must not be used.
Children from Y3 upwards should set their own password for the DEC Cloud and Google Docs, which should be a minimum of 6 characters and include either at least one capital letter or number. Generic or easily guessable passwords should not be used. (If teachers wish to keep a list of their classes passwords incase a child forgets theirs this should be treated as sensitive data and not printed out or written down on paper.)
All users must change their password during the first week of every term unless advised not to do so by the DEC's ICT team.
Curriculum
To be reviewed September 2017
Education and training for Parents will be held annually during the Autumn term.
Attention and time must be given to learning about and understanding potential dangers of electric sockets and the need for care when using the plugs / sockets on equipment.
The care and respect for all electronic equipment must be specifically included in any work / discussions around the Golden Rules and 6R's - Reflections
Children must be taught the correct procedures with regard to copyright laws (10%); sharing information - as per the DEC guidelines; and plagiarism APA guidelines to be followed when quoting a piece of text from another source.

E Safety Policy 2017

Becoming analytical applies also to the content of internet products and should be taught as a basic skill.

Health and Safety

Children will not be allowed to work with a laptop for extended periods of time - more than 1 hour without a break. Whilst they are working they should be encouraged to look around the room to exercise their eyes on a regular basis e.g. for 30 seconds every 10 minutes.

They will also be taught why it is important to limit the amount of time spent on individual devices including - wii, mobile phones, DS's, computers, ipads and ipods.

The children will be taught how to control the volume of headphones and why it is important to set your own reasonable volume level and that it is not appropriate to set it for others.

Equality

This aims to ensure that all staff will have safe and appropriate access to ICT equipment and through differentiation that all pupils will also have appropriate access to ICT equipment.

Monitoring

All staff will be responsible for the monitoring and review of this policy.

This Equal Opportunities policy is in line with the Departments policy on Equality.

Review September 2017