Introduction

The development and expansion of the use of ICT, and particularly of the internet, has changed learning in schools in recent years. ICT brings many benefits to teaching and learning.

At Heart of the Forest we take internet safety very seriously and it is our duty to keep our pupils safe whilst using technology. Through our e-safety policy, we must ensure that we meet our statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

Purpose

This policy is designed and intended to provide guidelines and working practices for the effective and safe use of the internet, email and other communications technologies in the school which pupils may be exposed, so that they have the confidence and skills to face and deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce risks.

The use of new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

• Access to illegal, harmful or inappropriate images or other content
• Unauthorised access to / loss of / sharing of personal information
• The risk of being subject to grooming by those with whom they make contact on the internet.
• The sharing / distribution of personal images without an individual's consent or knowledge
• Inappropriate communication / contact with others, including strangers and cyber-bullying
• Access to unsuitable video
• An inability to evaluate the quality, accuracy and relevance of information on the internet
• Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying, communication and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks.

Roles and Responsibilities

The role of the Governing Body
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.
• regular monitoring of e-safety incident logs
• regular monitoring of filtering / change control logs
• reporting to relevant Governors committee / meeting

The role of the school

Head Teachers and Senior Leaders
The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Co-ordinator.
• The Headteacher / Senior Leaders are responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues as relevant
• The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

ICT Co-ordinator/Business Manager
• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
• Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
• Provides training and advice for staff
• Liaises with the Local Authority
• Liaises with school staff
• Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
• Attends relevant meeting / committee of governors
• Reports regularly to Senior Leadership Team

Business Manager is responsible for ensuring:
• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
• That the school meets the e-safety technical requirements outlined in the Acceptable Usage Policy and any relevant Local Authority E-Safety policy and guidance
• The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
• Keeps up to date with e-safety technical information in order to effectively inform and update others as relevant
• That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher / Business Manager for investigation, action or sanction
• That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring:

• They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
• They have read, understood and signed the E-safety policy
• They report any suspected misuse or problem to the ICT Co-ordinator for investigation, action and sanction
• Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
 • E-safety issues are embedded in all aspects of the curriculum and other school activities
• Students / pupils understand and follow the school e-safety and acceptable use policy
• Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• They monitor ICT activity in lessons, extracurricular and extended school activities
• They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
• In lessons where internet use is pre-planned students / 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.

The role of the designated teacher
Is trained in e-safety issues and aware of the potential for serious child protection issues to arise from:

• Sharing of personal data
• Access to illegal or inappropriate materials
• Inappropriate on-line contact with adults or strangers
• Potential or actual incidents of grooming
• Cyber-bullying

Students / pupils:
 • Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils)
 • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
• Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyberbullying.
• Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

• Accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

• In lessons where internet use is pre-planned, 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, e.g. using search engines, 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, student's may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable, with clear reasons for the need.
• 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.

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• 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.
• Staff 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 students / pupils are carefully selected and comply with good practice guidance on the use of such images.

• Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
• Pupil's work can only be published with the permission of the pupil and parents and carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

• Fairly and lawfully processed
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate
• Kept no longer than is necessary
• Processed in accordance with the data subject's rights
• Secure
• Only transferred to others with adequate protection

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
• Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, USB stick or any other removable media:
• The data must be encrypted and password protected
• The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
• The device must offer approved virus and malware checking software
• The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

<u>Unsuitable / inappropriate activities</u>

Heart of the Forest School believes that the activities listed below would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred

- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling
- On-line shopping / commerce
- File sharing
- Use of social networking sites

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office. The Headteacher or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Pupils should not place personal photos on any social network space without considering how the photo could be used now or in the future. Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Pupils should only invite known friends and deny access to others.

Managing filtering

The school will work in partnership with all relevant parties to ensure that systems to protect pupils are reviewed and improved. The Network Manager receives a weekly report web activity from the Lightspeed Web Filtering unit. If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing video conferencing

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

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.

The senior management team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Mobile phones will not be used during lessons or formal school time, unless as part of a lesson, where directed by a member of staff. The sending of abusive or inappropriate text messages is forbidden. There will be heavy sanctions imposed on those students who misuse camera phones.

The use by students of cameras in mobile phones will be kept under review. Games machines including the Sony Playstation, Microsoft Xbox/ PSP and others have internet access which may not include filtering. Care is required if there is any use in school or other officially sanctioned location (classrooms – only with supervised use or the Sensory studio – again only supervised used) Staff will be issued with a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

<u>Authorising Internet access</u>

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems. Secondary pupils must apply for internet access individually by agreeing to comply with the Pupil Acceptable Use Policy. Parents / carers will be asked to sign and return the Parent / Carer Acceptable Use Policy.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.

Communicating e-Safety

<u>Introducing the e-safety policy to pupils</u>
E-Safety rules will be posted in all rooms where computers are used. Pupils will be informed that network and internet use will be monitored. A programme of training in e-Safety will be developed. All staff will be given the School e-Safety Policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT 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 can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship. Staff are asked not to have pupils as 'friends' on social networking sites.

Enlisting parents' and carers' support
Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school web site. The school will maintain a list of e-safety resources for parents/carers. Parents and carers will be expected to read and sign up to an acceptable use policy for their young person in school.

Equal Opportunities
The school supports the right of all staff and pupils to equal access and chances regardless of age, ethnicity, gender, social circumstances, ability / disability or sexuality.

Health & Safety
Health & Safety issues are described fully in the School Health & Safety Policy, which forms part of the guidance issued by the Local Authority. It is the responsibility of each adult to report health & safety issues without delay.

Professional Development
All staff are provided with training opportunities to deliver the curriculum including special requirements to meet the needs of pupils where appropriate. Training needs will be linked to Performance Management, staff interviews and the School Improvement Plan.

Ratified on:

Chair of the Governing Body: