Daventry Hill School

EE4A

e-Safety Policy

September 2016- onwards

Author- Charlotte Whysall

Introduction

DHS eSafety policy and guidance

DHS's intention in publishing an e-Safety Policy is not to impose restrictions that are contrary to DHS's established culture of openness, trust and integrity. This policy, supported by the acceptable use agreements for staff, Governors, visitors and learners is designed to protect the interests and safety of the whole DHS community. All users need to be aware of the range of risks associated with the use of ICT and related technologies.

Roles and Responsibilities

The Headteacher and Governors are responsible for ensuring that the policy and associated practices are embedded and monitored.

The Headteacher may nominate an e-safety coordinator. If no e-safety coordinator is nominated, the Headteacher will be deemed to be responsible for e-safety.

All elements of this policy apply to The Trust, Governors, employees, contractors, consultants, and other workers at DHS, including all personnel affiliated with third parties. It also applies to members of the public who use or connect to DHS equipment. This policy applies to all equipment that is owned or leased by DHS and the use of other devices to access the DHS network.

Any employee found to have violated any aspect of this policy and guidance may be subject to disciplinary action under DHS's Disciplinary Procedure, up to and including termination of employment. All staff will be asked to sign an acceptable Use agreement as part of their induction process.

Scope

This policy and guidance applies to both fixed and mobile internet technologies provided by DHS (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

These technologies are to be used for business purposes in serving the interests of our learners and staff in the course of normal operations.

DHS eSafety policy and guidance

- DHS has a framework for teaching internet skills in ICT/ PHSE lessons

- DHS provides opportunities within a range of curriculum areas to teach about e-Safety.

- Educating students on the dangers of technologies that may be encountered outside DHS is carried out informally when opportunities arise and formally as part of the e-Safety curriculum.

- Students are made aware of the relevant legislation when using the internet such as data protection and intellectual property, which may limit what they want to do but also serves to protect them.

- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

- Students are made aware of the impact of online bullying and of how to seek help if they are affected by these issues. Students are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. Learning Mentors parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ Child Exploitation and Online Protection (CEOP) report abuse button.

- Students are taught to evaluate materials critically and to learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

- DHS endeavours to create a consistent message with parents of all students. However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues. Where a pupil has additional needs in respect of social understanding, careful consideration should be given to group interactions when raising awareness of e- Safety. Internet activities must be planned and well managed for these children and young people.

DHS eSafety policy and guidance

Parental Involvement

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the School. Please see Appendix 2.

- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on an School website). Please see section 10.

- The School disseminates information to parents relating to e-Safety where

appropriate in the form of:

Information and celebration evenings; Posters; Website/ Learning Platform postings; Newsletter items.

All users are responsible for implementing password security in all aspects of creating, protecting and managing passwords. Passwords for DHS systems must be created and managed in accordance with this policy.

Password Disclosure Users must not disclose their passwords to anyone.

Users must not write their passwords down under any circumstances.

Unauthorised password disclosure is deemed a serious security matter and may be dealt with under the DHS's Disciplinary Procedure, up to and including termination of employment.

Shared Passwords

There may be rare occasions when it is necessary to share a common password between more than one user, if having individual usernames and passwords is operationally unacceptable, such as where the sharing of equipment is required, and the logout and login times required to swap users are unacceptable.

Any such arrangement must be authorised by the SLT.

All access to line of business applications, including email, will be gained through the use of individual logins which will have to be entered by each user independently.

Data Security

DHS eSafety policy and guidance

The accessing of School data is something that DHS takes very seriously. Any data shared with an external body must be subject to a data sharing agreement approved by the Head Teacher.

Staff must be made aware of their responsibilities when accessing School data.

They must not:

- access data outside of School, except when entering assessment data;
- take copies of the data;
- allow others to view the data;

- Edit the data unless specifically requested to do so by the Headteacher
- Leave the MIS open for students to view;
- Leave their workstations unlocked when leaving the classroom;
- Allow a student to use the classroom PC; and
- Share staff passwords or store passwords insecurely.

Acceptable Usage

Effective security is a team effort involving the participation and support of every DHS employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Managing Email

The Schools email system must not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any DHS employee should report the matter to their Line Manager immediately. Any breach of this eSafety policy may be dealt with under the DHS's Disciplinary Procedure, up to and including termination of employment.

8.1 Personal Use.

Using a reasonable amount of School resources for personal emails is acceptable, but non-work related email must be saved in a separate folder from work related email. Sending chain letters or joke emails from an DHS email account is prohibited.

Monitoring

School employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. DHS may monitor messages without prior notice. DHS is not obliged to monitor email messages.

Email Forwarding Policy

DHS employees are provided with an DHS email account. Employees are not permitted to use personal email accounts for DHS business. Unless approved by an employee's Line Manager,

DHS email will not be automatically forwarded to an external email address.

Social networking / Web 2 Technologies

DHS does not discourage staff and students from using such services in their own time. However, all should be aware that DHS will take seriously any occasions where the services are used inappropriately. If online bullying or harassment is found to have taken place, these will be dealt with in accordance with the DHS Harassment and Bullying policy.

It is important to recognise that there are also issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage staff and students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Any serious misuse of Social Networking sites will be dealt with in accordance with the DHS Disciplinary policy. Guidance is provided below in respect of Facebook and Twitter. The same principles should be applied to other social networking sites such as WhatsApp and Snapchat. This list is not exhaustive.

Facebook/Twitter

Staff may use Facebook/Twitter in their own time using their own IT assets. However:

- Under no circumstances should pupils or ex-pupils under the age of 18 be accepted as a friend. Failure to follow this will result in disciplinary action being taken. If a child requests a member of staff as a friend then the child's parents must be informed.

- Staff are asked to use extreme caution if a parent makes contact through Facebook. In the event of communicating with a parent or adult associated with a child who attends the school, an employee must not make any comments about students, staff or parents.

- Any statements or status remarks must not contain any comments about DHS, the School, staff, parents or students.

- Teaching Staff should not use DHS equipment to access social networking sites as part of their work unless prior permission has been granted by their Line Manager. .

Publishing pupil's images and work

On a child's entry to the School, parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the School web site;
- on the School's Learning Platform/VLE;
- in the School prospectus and other printed publications that the School may produce for promotional purposes;
- recorded/ transmitted on a video or webcam;
- in display material that may be used in the School's communal areas;
- in display material that may be used in external areas e.g. an exhibition promoting the School; and
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.) This consent form is considered valid for the entire period the child attends the School unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by the person with parental responsibility to be valid. Students' full names will not be published alongside their image. Email and postal addresses of students will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. No photos should be uploaded to website or put in any publications without prior checking with the Headteacher or nominated responsible person at the School. Only DHS or the nominated responsible person at the School has authority to upload images to the site. If links to Youtube are provided a disclaimer must state that this link is to an external website and that DHS is not responsible for the content of external sites.

Storage of Images

Images/ films of children are stored on the School's network.

Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.

Rights of access to this material are restricted to the teaching staff and students within the confines of the School network/ Learning Platform.

Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or DHS owned, that may connect to or access the information systems at

DHS.

.

Mobile technologies, including Removable Media Devices

Removable media devices, including laptops, mobile phones, tablets and USB memory sticks are particularly vulnerable to loss and theft due to their size and portability. Users must take all reasonable precautions to prevent a security breach. Approval for access to, and use of, mobile computing and removable media devices must be given by your Line Manager. Should access to, and use of, mobile computing and removable media devices be approved, the following sections apply and must be adhered to at all times.

Special care must be taken to physically protect the removable media device and stored information from loss, theft or damage. Anyone using removable media devices to transfer information must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.

Only information that is authorised and necessary to be transferred should be saved on to the removable media device. Users should note that information that has been deleted can still be retrieved.

Removable media devices must not be used for archiving or storing records as an alternative to other storage equipment.

Non-DHS owned removable media devices must not be used to store any information used to conduct official DHS business, and must not be used with any DHS owned or leased IT equipment unless authorised by DHS SLT.

It should be noted that if a user loses or has a mobile device/tablet stolen which contains unencrypted personal data owned by DHS, they may be liable to prosecution under the Data Protection Act 1998.

Misuse or Infringements/Inappropriate material

All users must be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-safety co-ordinator. The e-safety coordinator must record the incident on the e-safety log. This incident log must be monitored termly by the Headteacher.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety co-ordinator. Depending on the seriousness of the offence further action taken may include:

- investigation by the Headteacher/ Governing Body;
- immediate sanctions, possibly leading to exclusion/dismissal; or
- involvement of police for very serious offences. Users are made aware of sanctions relating to the misuse or misconduct through inductions (staff) and ICT lessons (students).

Computer Use

Appropriate measures must be taken when using computers to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorised users.

Employees using computers must consider the sensitivity of the information that may be accessed and minimise the possibility of unauthorised access.

Appropriate measures include:

- Restricting physical access to computers to only authorised personnel;
- Securing computers (screen lock or logout) prior to leaving an area to prevent unauthorised access;
- Enabling a password-protected screen saver with a short timeout period to ensure that computers that were left unsecured will be protected;
- Ensuring computers are used for authorised business purposes only;
- Never installing unauthorised software on computers; and
- Ensuring that monitors are positioned away from public view. If necessary, privacy screen filters or other physical barriers to public viewing will be installed.

Clear Screen

All users are expected to log off from their PCs/ laptops when left for long periods and overnight.

When leaving their desk for lunch or to attend a meeting, users should lock down their screen using Ctrl, Alt, Del and then selecting Lock Workstation. DHS systems will do this automatically after 15 minutes; however taking this measure will further reduce any security risk.

Mobile devices through which access to the network can be obtained, for example Ipads, should be PIN protected, set to power off after a period of within 5 minutes and switched off when left unattended. These devices should be stored securely when not in use.

Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher.

Review

This policy will be reviewed every three years, or when there are changes to relevant legislation.