VICTORIA DOCK PRIMARY SCHOOL

E-SAFETY POLICY

Working together for your children

Updated: Summer, 2016

To Be Reviewed: Summer, 2017

Introduction
E-Safety describes the use of new technologies involving mobile devices and the internet safely. Under this umbrella we aim to educate pupils about the benefits of using emerging technologies as means of collaboration and production whilst maintaining an emphasis on awareness and evaluation of risks related to these new technologies.

The school's E-Safety policy operates in conjunction with other school policies: Behaviour, Safeguarding, Bullying, Data Protection and PSHCE.

Our E-safety Guidance and Acceptable Use Policies have been written by Victoria Dock Primary School. They build upon the Hull City Council's (HCC) E-safety Policy and government guidance and are in accordance with Hull Safeguarding Children Board's Guidelines and Procedures which can be accessed via http://www.proceduresonline.com/hull/scb/ It has been agreed by Antonia Saunders (Headteacher) and approved by the governing body.

E-Safety teaching and maintenance can be seen across school at different levels:
- Responsible and secure use of ICT by all adults as an example to pupils.
- Clear and published policies regarding aspects of administration and curriculum.
- Safe and secure internet access provided by KC and filtered through Smoothwall with management from the ICT technician.

Learning and Teaching
Members of the school community including students, staff, governors, parents and carers are educated on the benefits and risks of using new and emerging technologies in different ways. Safe and responsible behaviour when using these technologies is promoted throughout school by a number of means:
- Specific E-Safety lessons which may fall into the category of PSHCE.
- Assemblies and whole-school activities such as Safer Internet Day.
- Reactive sessions and workshops when opportunities/risks arise.
- Use of age appropriate internet tools to support learning.
- Reminders of personal accountability through an end-user Acceptable Use Policy (AUP) which is displayed at each login.
- Clearly visible methods of reporting inappropriate content/behaviour for in and out of school.

Staff Training
Staff receive regular E-Safety training in the form of inset sessions and are updated to new and emerging risks where appropriate.
Staff are made aware of responsibilities regarding E-Safety and safeguarding pupils, whilst also maintaining awareness of reporting procedures.

ICT Systems
Victoria Dock Primary School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will

never occur via a computer.
Neither Victoria Dock Primary School nor HCC can accept liability for the material accessed, stored or distributed or any consequences resulting from Internet use.
Victoria Dock Primary School should audit digital technological use to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.
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 will be reviewed regularly.

Staff are responsible for ensuring that ICT systems are used safely and securely by themselves and pupils in their care. Devices and access to technologies are controlled and moderated by the ICT technician. Anti-virus and system tools are kept up to date at all times to ensure appropriate protection.

Access to technologies is controlled by school and varying levels of supervision and access are dispensed by the ICT technician.

All users sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and type of access. This policy acts as a reminder to the rules, regulation and guidelines to using school technology.

At Key Stage 1, pupils will access technology through the use of an individual user name and an open password. Use of extended networks such as the internet is controlled and monitored by the class teacher and supervising adults.

At Key Stage 2, pupils have an individual user name and password which is kept secure. They digitally sign an AUP with every login.

Staff members access technology using their own secure user name and password and abide by a staff AUP at all times, including ensuring they lock workstations when not using them.

E-Mail
Staff and pupils have an allocated email address provided by Gmail and monitored by the ICT technician. Use of personal email accounts for transfer of school documentation is prohibited.

All email contact with parents, carers and other stakeholders is done through the use of official school email accounts and it is encouraged that other relevant staff are copied in.

Pupils are reminded to report any inappropriate email content/behaviour using clearly visible reporting procedures.

Publishing
Victoria Dock Primary School will control access to social media and social

networking sites. Children will be advised never to give out personal details of any kind which may identify them and/or their location to persons unknown or through unsecured sites. Examples would include their real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Children should be advised not to place personal photos or videos on any unsecured social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail (such as a school crest) in a photograph or video which could identify the child or his/her location.

Organisational blogs or social media sites should be password protected and run from the organisational website with approval from the Senior Leadership Team/Senior Manager.
Employees/volunteers should be advised not to run social network spaces for children's use on a personal basis.

If personal publishing is to be used with children and young people then it must use age appropriate sites suitable for educational purposes and the site should be moderated by organisational staff. They should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children should be encouraged to invite known friends only and deny access to others by making profiles private.

Children are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Copyright must be held by the school or attributed to the owner where permission to reproduce has been obtained.

Permission from parents/guardians, in the form of an agreement signed on school enrollment, must be obtained before publishing photographs/video.

Official school accounts must be used to post all content. No personal accounts for any reason.

In addition to these guidelines, staff are to ensure that any online presence they hold such as on social networks or blogs is in keeping with their professional standards. Staff members must not engage in any activity which would be damaging to the school such as posting inappropriate content or participating in online messaging about sensitive or damaging issues.

Staff must be aware of privacy settings on personal accounts and should ensure that reasonable safeguards are put in place to prevent pupils making contact with these accounts. Staff who hold an account should not have pupils as 'friends' or contacts unless the account has been opened for the specific official use of school for home links and has been approved by school leadership.

Filtering
Internet use is filtered through the use of a Smoothwall filter which is maintained and monitored by the ICT technician. Pupils and staff are reminded at login of their responsibilities regardig safe and secure use of technology and clear reporting procedures are in place through the use of desktop short cuts to report inappropriate content and also key members of staff being prominent and available to pupils as an alternative. Either method of reporting must reach the E-Safety leader. The school will report incidents to the relevant agencies such as the ICT technician, filtering provider, local authority or CEOP.

Exceptions to the list of websites filtered can be made on the discretion of the ICT technician in conjunction with guidance from E-Safety leader and the Senior Leadership Team (SLT). Continuous evaluation of usefulness and appropriateness of digital content is a skills which is promoted and pupils are encouraged to play an active role in this.

Emerging Technologies
New and emerging technologies are regularly examined regarding their educational purpose and corresponding risk. New technologies are evaluated before being used in school.

Mobile and Personal Devices
Personal mobile phones and devices should not be brought into school by pupils. In the case that these devices are brought in, school can not accept responsibility for them and their use, however they will be confiscated to ensure pupils are safeguarded against risks associated with their use.

In the case of events open to parents and carers, adults are permitted to take photos and videos of their own child and are reminded to not share these on social networking sites.

Mobile devices made available for pupils use such as iPods are used in accordance with the AUP signed by pupils and are used under the supervision of members of staff. Where possible, use is limited to the specific features required.

No images or videos should be stored on any personal mobile devices owned by members of staff. Photos and videos should only be created and stored on school-owned devices. Similarly, staff must not use their personal devices including mobile phones to contact pupils or their families.

Internet Access
Victoria Dock Primary School will maintain a current record of all staff/volunteers,

children and young people who are granted access to the organisation's electronic communication systems..
All staff/volunteers must read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resource.

For Foundation stage children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Children in KS1 and KS2 must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy (AUP). Parents/carers will be asked to sign and return a consent form for children and young people's access.
Parents/carers will be informed that children and young people will be provided with supervised and unsupervised Internet access, but must comply with the AUP at all times.

As with use of devices, access to the internet is controlled by school and varying levels of supervision and access are administered by the ICT technician.

The AUP is signed digitally on each login and acts as a reminder of the rules and regulations required for school use of the internet. Parents are required to sign the home-school agreement prior to pupils being granted internet access at school.

Data Protection
The school complies with the Data Protection Act 1998 and all personal or sensitive information is stored in appropriately closed/locked storage. All computers which have access to sensitive information should be locked (Ctrl+Alt+Del) when unattended.

Sensitive information is stored on separate servers and access is controlled by the ICT technician, operating on a privilege basis.

Personal and sensitive information must not be taken away from school by any means such as USB drives, cloud storage or email transfer without suitable encryption. Similarly, such information should not be stored on any personal devices such as laptops without authorisation from SLT and proper encryption.

Users accessing sensitive and personal information when on or off site should be vigilant to who can read the information.

Approved Cloud Services
Personal or confidential information should be kept on school servers where possible; however, when it is necessary to use cloud services for the storage of such information, for collaboration, the following list of services is to be used only:

- Google Apps for Education
- Seesaw

Assets

- Details of all school owned hardware will be recorded in a hardware inventory both in hard copy and electronically.
- Details of all school owned software will be recorded in a software inventory both in hard copy and electronically.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (amended) Regulations 2007. See Environmental Agency website for details

Parental Support

Parents' attention is drawn to the school E-Safety policy and regular updates to content are maintained in different ways:

- Notes in newsletters.
- School website.
- Parent workshops.

Parents are kept involved with pupil's E-Safety education and must sign the home-school agreement prior to pupils being granted internet access at school. Parents are also reminded of the AUP which all pupils adhere to. This is posted on the school website.

Response to incident of concern

Online sexual exploitation

Victoria Dock Primary School will be vigilant in relation to child sexual exploitation and online grooming. Staff/Volunteers will be made aware of the organisations protocols and responsibilities in relation to online grooming including how and to whom to share information and concerns.

Victoria Dock Primary School will follow HSCB 'Incident Log' to record any issues and will report any concerns about a child's safety to Children's Social Care.

Victoria Dock Primary School will develop approaches to educate children, young people and parents on the dangers of online grooming and sexting.

Sex and Relationship Education and/or PHSE may be an opportunity to explore issues including consent, sexting, appropriate relationships, pornography use and protective steps children and young people can take online.

Sexting

Victoria Dock Primary School will make children aware of the risks associated with the creating, storing and sharing of images of a sexual nature. Clear procedure, adhering to the 'Response to Risk Flowchart' (Below), is in place to support anyone affected by 'sexting'; including appropriate referrals to Children's Social Care and/or the Police and organisational responses including involvement of Child Protection Co-ordinators and E-safety leads.

Cyber-bullying

Cyber-bullying (along with all forms of bullying) will not be tolerated in Victoria Dock Primary School. Full details are set out in Victoria Dock Primary School's policy on anti-bullying. All incidents of cyber-bullying reported to Victoria Dock Primary School will be recorded. Children and young people, staff/volunteers and

parents/carers will be advised to keep a record of the bullying as evidence. Victoria Dock Primary School will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

An important element of E-Safeguarding is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff/volunteers, children and young people have a responsibility to report e-safety or e-security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents in an incident log which is kept in a secure location. The chain below demonstrates the key members of staff for which a cause for concern is dealt with in school.

Michael Hague – E-Safeguarding Officer
Emma Boyes – Child Protection Officer
Claire Juggins – Deputy Head Teacher/Safeguarding Officer
Antonia Saunders – Head Teacher

Response to Risk Flowchart