VICTORIA DOCK PRIMARY SCHOOL

E-SAFETY POLICY

Working together for your children

Updated: Summer 2019

To Be Reviewed: Summer 2020

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 a 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 PSHE.

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.
- Monitoring reports generated by Esafe Global to highlight possible breaches or incidents.
- Safe and secure internet access provided by KC and filtered through Smoothwall with management from RM Education.

This policy applies to all aspects of the school, including out of hours provision e.g. clubs run by staff and outside providers.
This policy links to other policies and supports the school's safeguarding, health and safety, anti-bullying, child protection and internet acceptable use policies.

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 follow the South West Grid for Learning (SWGfL) Digital Literacy scheme of work.
- 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 in appropriate areas around school.
- 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 Hull City Council (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 Computing Subject Leader and RM Education. Antivirus and system tools are always kept up to date to ensure appropriate protection.

Access to technologies is controlled by school staff and varying levels of supervision and access are dispensed by RM Education, along with class teachers.

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 of the rules, regulations and guidelines to using school technology.

Pupils have an individual username and password which is kept secure. AUPs are

visible for parents to sign at each autumn parents' evenings.

Staff members access technology using their own secure username 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 RM Education. 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 or approved means such as Seesaw or Classdojo and it is encouraged that other relevant staff are copied in where appropriate.

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 enrolment, must be obtained before publishing photographs/video.

Official school accounts must be used to post all content. No personal accounts should be used 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 contacting 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 RM Education. Pupils and staff are reminded of their responsibilities regarding safe and secure use of technology and clear reporting procedures are in place using desktop shortcuts 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-Safeguarding Officer. The school will liaise with the relevant agencies such as RM Education, Smoothwall, E-Safe, the local authority or CEOP when responding to incidents.

Exceptions to the list of websites filtered can be made on the discretion of the Computing subject leader in conjunction with guidance from E-Safeguarding Officer

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.

MONITORING

Whilst directly accessing technology, children are monitored physically by their teacher and other members of staff present. This requires staff to be present and vigilant and reflects our school's current situation: few e-safeguarding incidents lead to a conclusion of low risk. This will be amended if circumstances change.

All internet traffic is logged within the Smoothwall Admin Console and is accessible to the Computing subject leader or RM Education on request. Staff and children enrolled at Victoria Dock Primary School have their internet access and history logged within this system. Guests to the school, logged in to the VDPS_Guest wifi network, have their history logged against the personal credentials they provide at login and their IP address.

Incidents which involve violation of the filters (see above section: Filtering) are identified by a the software, E-Safe, which the school uses to trigger a notification to both the Computing subject leader and headteacher for action (See below section: Response to Incidents of Concern). The school uses software from ESafe Global to monitor internet use of all users on the school network, reporting breaches and incidents to the E-Safeguarding officer at appropriate intervals depending on the severity of case.

With the exclusion of incidents requiring action, internet history and access logs are reviewed termly by the Computing subject leader and RM Education.

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.

Children are to be involved in the monitoring and evaluation of emerging technologies (including apps) through regular 'open floor' sessions involving individual classes and the e-safeguarding officer.

MOBILE AND PERSONAL DEVICES

<u>Pupils</u>

While we acknowledge a parent's/carer's right to allow their child to bring a mobile

phone to school, Victoria Dock Primary School discourages pupils from bringing mobile phones to school. In general, pupils should not bring valuable items to school as they can be lost or stolen. Parents are reminded that in cases of emergency, the school office remains a vital and appropriate point of contact.

Where parents allow children to bring a mobile phone to school, they do so entirely at their own risk. The school accepts no responsibility for any loss or damage whilst the phone is on school premises. If a pupil brings a mobile phone to school, they must hand it into the office and collect it at the end of the school day.

If a pupil is found taking photographs or video footage with a mobile phone of either, other pupils or members of staff, this will be regarded as a serious matter and disciplinary action will be taken in accordance with the school's behaviour policy.

Staff

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones and personal devices within our school setting, which is agreed to by all users.

- Staff are not permitted to use mobile phones or personal devices whilst carrying out any duty that involves supervision or contact with children (with the exception of trips and visits where mobile phones may be used to facilitate the health and safety of the members of the party).
- Staff will not use their mobile phones or personal devices in pupils' presence unless prior permission has been obtained from the Headteacher.
- Staff are not at any time permitted to use recording equipment on their mobile phones or personal devices, for example: to take photographs or videos of children, or share images and will only use work-provided equipment for this purpose.

Parents

While we would prefer parents not to use their mobile phones while at school, we recognise that this would be impossible to regulate and that many parents see their phones as an essential means of communication . We therefore ask that parents' usage of mobile phones, whilst on the school site is courteous and appropriate to the school environment.

We also allow parents to photograph or video school events such as shows or sports day using their mobile phones - but insist that parents do not publish images (e.g. on social networking sites) that include and children other than their own.

SMARTWATCHES

Personal fitness trackers and similar technology, which does not use cellular connectivity, are permitted but discouraged along with other valuable items as they can be lost or stolen.

Smartwatches and similar devices, which have their own means of cellular connectivity or internet access, are to be treated with the above guidelines (see Mobile and Personal Devices).

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 on each autumn parents' evening. 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 RM Education.

The AUP is signed at each autumn parents' evening 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.

<u>Guests</u>

Adults visiting Victoria Dock Primary School and requiring access to the internet are to gain access to the VDPS_Guest wifi network by logging in with their own personal details. These are then timestamped and logged for later reporting if necessary.

DATA PROTECTION

The school complies with the Data Protection Act 2018 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 RM Education, 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 hardcopy and electronically.
- Details of all school owned software will be recorded in a software inventory both in hardcopy 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 SUPPORTS

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 pupils' 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 AN 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 with 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.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our academy follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people,

2016.

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 cyberbullying 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 records 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/Computing Subject Leader
Claire Juggins – Deputy Head Teacher/Safeguarding Officer

Antonia Saunders – Head Teacher

Response to Risk Flowchart

Response to and Reporting of an E-safety Incident of Concern