E-safety Policy

Approved By:	Full Governing Body
Date:	Oct 2022
Review Date:	Oct 2023

This policy reflects the views and discussions of teaching staff at Victoria Road School. It is designed to run alongside the Department of Education, Sport & Culture's Acceptable Use Policy.
Upon joining Victoria Road School, KS1 children are made aware of the Acceptable Use Policy (Appendix 1) and KS2 are expected to agree to the 13 points raised in order to promote and adhere to a high standard of digital conduct.
The school's e-safety curriculum is designed to underpin the statements made in this policy.

Online

Access to the internet -
Children should always be supervised when using Computing equipment to browse the internet. There should be no unsupervised use of Computing equipment at break or lunchtimes. Teachers will use a number of strategies to manage children using the internet in lessons including but not limited to:

- providing a range of suitable websites e.g. QR codes
- walk around and discussion with children about what they are viewing
- independent learning activities will be monitored by staff
- if not all children on laptops can be monitored then they should not be on internet ready equipment, if not 1:1, then group/paired learning may be more appropriate

Staff will be proactive in monitoring what children are doing on the internet, they will discuss what they have viewed, highlight safer searching and image filters, look for minimised windows and tabs. All staff will be aware of the **Internet Inappropriate Content Protocol** (Appendix 2) to follow if a child views something inappropriate on the internet.

Web filtering:
The Department of Education, Sport & Culture and Government Technology Service (GTS) have web filtering set up in school and this should block most inappropriate content, sometimes things do get through and the **Internet Inappropriate Content Protocol** (appendix 2) should be followed if a child views something inappropriate on the internet. Children should be aware of their role in reporting any inappropriate content to staff. Staff should be mindful of difference in levels of disgust amongst children.

Use of pupil devices to bypass web filtering:
3G and 4G pupil devices are not presently routinely allowed into school - see the Personal Mobile Device Policy. With the recent developments in mobile technologies and Virtual Private Networks (VPNs), devices capable of accessing these services are not typically allowed into school, unless prior consent is given for a learning purpose by a Senior Leader.

Use of School Website and Class Dojo:
It is agreed that whole school events will be posted on Class Dojo as well as anything that staff feel should be seen and celebrated by parents/carers. This website is to publicise and promote our school, and to share key information relation to staffing and policies. Correspondence with school through the website's contact function is not routinely monitored and we strongly advise parents to contact the school by phone or the enquiries email. Class Dojo can be used to communicate with parents but this is not monitored during school hours.

Social networking sites:
Whilst we do not encourage (and actively discourage) the underage use of social networking sites such as Facebook, Twitter, Snapchat and Instagram we will respond to pupils requests for education in how to help them make these accounts more secure. We make pupils aware of the dangers associated with social networking sites as part of our e-safety curriculum. We aim to educate parents through our school website and School Story on Dojo. In addition to these channels, we also strongly recommend the use of the 'Safer Schools' mobile application by staff, children and parents/carers as a first point of call for advice on social networking sites/current issues.

Appropriate behaviour (including cyberbullying):
Cyber bullying for children will be dealt with as per our Anti-bullying and Behaviour policy. Staff should model good practice in terms on their behaviour when using technology. There is an expectation that parents will model appropriate behaviours online in accordance with the school's Acceptable Use Policy. Additionally, the 'Safer Schools' mobile application has accessible advice pages on cyberbullying and appropriate behaviour on the internet.

Online Gaming:
The school provides guidance to parents/carers via the school's website on the topic of online gaming and how to protect their children in this space. The website has a dedicated 'E-Safety' section on the website that is updated by SLT, the Computing Co-Ordinator and the student 'Digital Leader' team. Specific advice for gaming and specific games can be accessed through the 'Digital Safety' page on the Safer Schools app. This section is kept up to date with the most recent content for new games which children may be engaging in.

Personal Data

All staff laptops are to be password protected and are encrypted to ensure content on them is secure.

School's storage and use of images:
The school uses the Department of Education, Sport & Culture's wording on its photograph/video disclaimer letter and this is sent out via schools Information Management System (IMS) when a child starts at the school and can be updated as and when appropriate. Records of children who may/may not be photographed/videoed are kept by class teachers and also centrally on the IMS.
When taking photographs all staff should follow these guidelines:

- Personal devices (eg phones) should not be used for taking photographs of children. (If for any reason this is necessary (and agreed by SLT) then photos must be downloaded onto a secure space using a school device and must be deleted immediately from the

staff members personal device). Also staff are not permitted to have virtual 'Cloud' backups of this specific data.
- Photos on devices should be removed as soon as they are no longer required.
- Staff should delete photographs of children who are no longer at the school unless the photographs are being kept as examples of particular educational practice or similar.
- The use of USB 'pen drives' for photographs by staff or children is not allowed.
- Photographs must only be stored on encrypted staff devices or the secure cloud server.

Holding sensitive data:
Sensitive data is any information stored that allows children or groups of children to be identified and may include: names (first and surnames), DOB, addresses, phone numbers, class lists, reports, Child protection records, passwords, staff observations & performance management records, SEN register etc.

No sensitive data should be placed on USB drives, their use is not allowed in school. It is the responsibility of all members of staff to ensure they have secure passwords set on files/programs which contain sensitive information. Like shredding paper copies, consideration should be made to emptying trash regularly.

Sending sensitive data:
When staff are required to send personal information regarding staff/children, they are required to do so in accordance with the school Data Protection policy.
When these occasions arise where data transfer is necessary, this is done so through an encrypted/password protected document and transfer method, such as (but not limited to); staff email servers, secure cloud server. Passwords to the documents should be sent via a separate email.

Students use of personal information:
Children will be educated about personal information as part of the school's e-safety curriculum.

Accounts:
From Year 3 upwards children are given access to their own 'Google' account for educational purposes with consent from parents and guardians. This involves access to: GMail, Drive (cloud storage) and shared word processing, presentation tools.
This requires children to have their own account which is password protected through an internal account structure managed by Government Technology Service. Passwords should be regularly changed by children - good practice and education is provided in line with our school e-safety curriculum and account etiquette should be modelled by all staff in the school.
If a child believes their accounts have been compromised, they should inform their teacher immediately and change their password.

Curriculum

Education and training for students and parents:
The school's e-safety curriculum is designed to raise awareness and give children the knowledge and understanding they need to be safer online, reducing the risk. The curriculum is progressive from Reception to Year 6. Differentiation of access to the curriculum and differentiation of the curriculum will be considered by teachers with consideration of varying needs. The curriculum has been designed to appeal to and cater

for a range of differing learning styles. The school's e-safety curriculum will be flexible to reflect and meet the learning needs of the children in each class and the continuous development of technology.

Safer Schools Application:
In line with the Department of Education, Sport & Culture, Victoria Road Primary School engages in the use of the 'Safer Schools' mobile application.
This app has been custom designed to keep parents, pupils and staff members at school aware and up to date of some of the most current issues that children are finding, in regard to the digital world. The Safer Schools app aims to help the Island's school communities better protect themselves by having safeguarding information at their fingertips.

The school will, in conjunction with Digital Leaders, highlight related events such as Safer Internet Day which will be used to heighten awareness and create opportunities for open discussions around issues children may be facing online, with the overall aim to educate children on digital good practice.
In addition there is a dedicated e-safety area on the school's website which is updated periodically.

All parents and carers, children and staff are strongly advised to download and make use of the Safer Schools application.

Devices

Use of handheld devices (including mobile phones):
The Mobile Device Policy outlines the procedures for handheld devices in school.
If a teacher does wish to allow devices into school for a specific learning experience (eg trip) they should liaise with the Computing Coordinator/SLT as appropriate.

Sanctions for misuse

Including confiscating items:
Personal devices will be confiscated if misused. Technology privileges may be removed in line with **Internet Inappropriate Content Protocol** (appendix 2)**.**

Clarity over accidental, deliberate or illegal access to inappropriate material:
See **Internet Inappropriate Content Protocol** (appendix 1) for this. This should be reported to a member of SLT to be recorded on Arbor as log either as 'Inappropriate content' or 'misuse'.

Sanctions for bullying, harassment, sexual exploitation, racial or hate motivated incidents:
Will be in line with the school's anti-bullying and behaviour policies.

Staff responsibilities

Modelling good practice:
Staff will make parts of their everyday practice explicit to the children to reinforce good e-safety practice. eg deleting photos, using safe search filters for images, having a screen saver set and entering a password.

Adhering to policies & knowing when to escalate e-safety issues:
All staff will be aware of and follow the Acceptable Use Policy. They will also familiarise themselves with the **Internet Inappropriate Content Protocol** (appendix 2) and other parts of related policies. (eg anti-bullying/behaviour). A log of internet incidents will be kept on the IMS and monitored by SLT.

Maintain a professional level of conduct in their personal use of technology both within and outside:
See point 6 on AUP as this has clear instructions for staff. The following policies also apply to all staff: IOM Government - Electronic Communications and Social Media: Policy, Standards and Guidelines , IOM Government - Guidelines for the Use of Electronic Communications and Social Media.

Take personal responsibility for their professional development in this area
It is the responsibility of staff to highlight and address their own training needs in relation to Computing and e-safety. The Computing coordinator, department and other staff will aim to provide training as appropriate. Staff are expected to make use of the Safer School's app as a channel for maintaining their professional development and knowledge in order to best support the children in their care. Staff have sole access to specific areas of the application that are purpose build for this function.

Reviewing Policy
This policy will be reviewed on a 3 year basis or as the need arises and will be highlighted to all staff at the start of each year. The policy will be highlighted to new teaching staff as part of the schools induction policy.

This policy is in conjunction with:
- Acceptable Use Policy
- Anti Bullying Policy
- Behaviour Policy
- DESC Acceptable Use Policy
- Personal Mobile Device Policy

Updated - Sep 2022
Approved by governors - Oct 2022
Review - Oct 2023

Appendix 1

ICT Acceptable Use Agreement

You will **not** use school ICT equipment until you have signed this document. These rules help to keep everybody safe and allow us to be fair to others.

These rules apply to all equipment in school.

1. **I will ask permission from a member of staff before using any devices.**
2. **I will not use technology out of sight of an adult (not outside of classrooms/in shared spaces).**
3. **I am responsible for my behaviour when using devices and the internet.**
4. **I will treat all devices in school with respect and look after them.**
5. **I will make sure devices are stored safely and charged.**
6. **No device use is secret. All usage can be tracked and traced back.**
7. **I will keep personal information safe. This includes name, address etc.**
8. **I will ensure that school devices stay on 'DoEnetP' (network) at all times.**
9. **I will not make attempts to bypass the web-filtering system.**
10. **Devices and the internet are to be used for educational purposes only.**
11. **Keep all account passwords secret.**
12. **No unsuitable material. If I see any unsuitable content I will tell an adult straight away.**
13. **I understand that the ICT Co-Ordinator can monitor and track the use of school devices at all times.**

If I fail to follow any of these rules then my use of ICT in my school may be limited or completely stopped. My activities may also be reported to other people if necessary.

Name:

Signed (Pupil):

Signed (School):

Date:

Appendix 2

Internet Inappropriate Content Protocol

This policy outlines steps to be taken to prevent children from viewing inappropriate content on the internet and also outlines steps to be taken should this situation arise.
The Policy is taken from the Department of Education, Sport & Culture's guidance for Internet safety.

Children must be supervised at all times when using the internet and what they are viewing should be monitored.
This applies in all lessons and during any lunchtime or after school clubs. This supervision may be by talking to the children about what they are doing, viewing their screen during walk around.

Steps to follow in the event of child/children viewing inappropriate content on the internet.

If you notice a child viewing something unsuitable or a child reports that they have seen something unsuitable do **NOT** quit the browser, instead simply click the back button or minimise.
Talk to the children about what they have seen, what they were searching for and who saw it?
If there were others around who viewed/saw the content their names should be recorded.
It may also be useful to view the History to see what else the children have been looking at.

* Copy the URL (website address) into an e-mail and send this to GTS via a Helpdesk ticket who will block the site.
* Speak to a member of Senior Leadership Team and explain what happened and the circumstances.
* Log the incident with the aforementioned information using Arbor either as 'Inappropriate content' or 'Misuse'
*

The Head/Deputy head will advise what action is to be taken:

This may be to phone the parents to explain that their child has accessed an unsuitable site/image and your understanding of why/how (by accident, innocent or searching on purpose etc)
It should be pointed out to parents that schools have very effective internet filtering but that sometimes it is still possible to find unsuitable material. Parents may wish to know the nature of the viewing so that they can discuss/follow up this at home with their child.

A log of instances where children have viewed inappropriate content/images on the internet will be kept and all occurrences should be logged by a member of the Senior Leadership Team or the member of staff supervising the children at the time.