Isle of Man Department of Education
St Johns School

E Safety Policy

What is e-Safety?

E-safety is safeguarding children in a digital world - ensuring that they feel safe, that they understand the risks as well as the benefits of being online both in and out of school.

The DEC has an Acceptable Use Policy which provides clear information regarding all aspects of safety when using Department networks and equipment. St Johns Primary School will work within this policy.

Online

There is access to the Internet in school which is filtered and only when adults are present.

Social networking sites may not be used by children of Primary School Age.

The children have access to a secure online platform, ItsLearning. This is a secure platform which can only be accessed by other school children, education staff and members of the GTS team. Any online chats are closely monitored by teaching staff to ensure it is used appropriately.

Personal Data

All images taken in school will be stored on school servers and removed from all other equipment as soon as it is practical to do so.

Holding sensitive data will be restricted where practical to the school servers. When it is necessary to make use of data away from the school, users must be aware of issues to do with security and confidentiality when making use of the data, such as for assessment and report writing, e.g. laptops must be logged out when not being used and a security password (the default password must be changed to your own) should be enabled to gain any access to the device. Once the data has been used it must be stored, if necessary, back on the school server and deleted from personal laptops.

Pupils use of personal information should be limited to their own data used in their own personal area of the school network.

Passwords - Access to all equipment and corporate data will be by password.

Isle of Man Department of Education
St Johns School

E safety Policy

Curriculum

Education and training for pupils and parents.

The main elements of e-safety at Key Stage 1.

- Inappropriate images - what should children do if they come across an unsuitable image.
- Looking after equipment - how to handle equipment appropriately, including the use of electricity.
- Treating others responsibly - behaving well, including online.
- Gaming - look at the age ratings of games - they should be not too violent and they should play for a short time.
- Friends sites (social networking) - know age restrictions and that people may not be who they say they are.
- Personal information - what is personal information and why shouldn't we tell people.

TOP TIPS

1. People may not be who they say they are.
2. Be nice
3. Keep personal information private
4. tell a grown up that you trust if you get the "uh-oh!" feeling.

The main elements of e-safety at KS2.

These elements are in addition to & build upon the elements for KS1. The elements can be categorised into the following groups:

1) Content

- Dealing with nasty or unwanted comments.
- Dealing with junk mail, email attachments.
- Age inappropriate content that causes offence.
- Racist or biased content.
- Reliability of websites, pop up windows.
- Security risks of viruses, adverts and spam.

Isle of Man Department of Education
St Johns School

E safety Policy

2) Contact

- Chat rooms, gaming and social networking sites.
- Personal Online spaces. Keeping personal information safe – what is personal information? The potential dangers of posting details online.
- Cyberbullying, stalking and harassment that threaten psychological well being.
- Instant messaging/text messaging.

3) Conduct

- Understanding copyright and illegal downloading and plagiarism.
- Gambling
- Harassment and bullying.
- Creating inappropriate material including videos.
- Misleading information.

For older children, another category is

4) Commercial

- Understanding how credit cards are used online
- Abuse of details and scams (or cyber tricks)
- Mobile phone rates
- Advertising and sponsorship

'SMART' thinking is a useful way of judging what is appropriate and/or acceptable:

Safe Meeting Acceptable Reliable Tell

Devices

Use of handheld devices (including mobile phones).

Mobile phones may not be used by pupils during the school day. Phones brought to school are to be handed into the School Office at the beginning of the day and collected at the end of the day

Use of personal equipment may only be used with the express permission of the DEC ICT team. Enabling access to the school network is controlled by the DEC ICT team.

Isle of Man Department of Education
St Johns School

E Safety Policy

Sanctions for Misuse
If deemed necessary items will be confiscated if they are being used inappropriately. Personal devices brought into school will be taken to the School Office to be collected by the child's parent. Use of school equipment will be denied if necessary. Clarity over accidental access to inappropriate material should be reported to a class teacher. Deliberate or illegal access to inappropriate material will be dealt with using the sanctions listed here.

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

Staff Responsibilities

Staff have a responsibility to:

- Model good practise.
- Adhere to policies.
- Embed e-safety across the curriculum.
- Know how and when to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology both within and outside school.
- Take personal responsibility for their professional development in this area.

Vulnerable Groups

Provision for vulnerable pupils and parents to understand e-safety issues will be made by class teachers in consultation with SEN staff who are best placed to understand and know the needs of these pupils.

Isle of Man Department of Education
St Johns School

E Safety Policy

Unsuitable Sites & Images

Occasionally pupils will access unsuitable or inappropriate material on the Internet. The DEC provide secure, filtered web access but not all unsuitable material can be filtered out. For example, using Google image search, the 'thumbnail' images are not filtered but the sites they come from are. It is not possible to filter these thumbnail images without blocking 'Google Images'.

If a child finds an image or site that is inappropriate, They must be encouraged not to show it to their peers. They should not close the browser, but close the lid on the laptop, then tell the teacher who is supervising them. The teacher needs to ask the pupil what they were searching for and who saw the image. The teacher needs to keep the URL (website address) of the offending site and send it to the ICT Helpdesk for blocking. The teacher involved needs to inform their line manager and the parents informed. This usually happens by accident and sometimes the child is upset by it. Informing the parents of the nature of the image gives them the decision whether to discuss it further at home. If parents are not informed by the school, but by the child, parents can, quite rightly worry about the way the school handles these types of incident and the supervision of Internet access. If a child is wilfully trying to access unsuitable material, they are breaking the school's Acceptable Use Policy and we recommend that sanctions are enforced in alignment with the school's behaviour policy.

In summary -

1. Close the lid and notify the teacher
2. Copy and paste URL onto an email
3. Ask if other children have seen the image
4. Investigate what the pupil was searching for
5. Inform line manager
6. Inform parents including the nature of the image and if there was any blame on the child
7. Send email to help-desk for blocking

Responsibilities

St Johns Primary School has an AUP (Acceptable Use Policy), e-safety policy and a designated ICT co-ordinator. Their role is to develop and maintain an e-safe culture. The school's Headteacher and leadership teams will review the e-safety resources and the key issues involved. INSET training will be made available and, where possible, pupils will be included in decisions about what should be included. Our Anti-bullying Policy includes cyberbullying.

Written Spring Term Term 2017 (TW)
Shared with Governors April 2017

Reviewed September 2019