2020/21 Bulletin 40

EMMET HOUSE, MILLTOWN, DUBLIN 14
TEL: 01-283 8255 FAX:
01-269 5461
E-MAIL: info@jmb.ie
Website: www.jmb.ie

Staying Safe Online

1. Safer Internet Day 9th February 2021 – '*Together for a Better Internet*'.

Safer Internet Day (SID) is an EU wide initiative to promote a safer internet for all users, especially young people. It is promoted in Ireland by the PDST Technology in Education and Webwise.

#BeKindOnline Webinars the Irish Safer Internet Centre will host a series of free online safety webinars for parents and educators.

Further details available: https://www.webwise.ie/saferinternetday/

Follow on JMB Twitter

2. Online Platforms

DES Circular 74/2020 requires all schools to have an online platform in place to facilitate communications and remote teaching and learning. School management are reminded about the JMB's Advisory note on *Minimising Risk When Teaching Remotely* which remains very relevant to the safe operation of online platforms, such as Office365 Education or GSuite for Education. For example, best practice recommendations include:

- only approved and contracted solutions should be used (i.e. those approved by school management with an appropriate agreement in place between school and service provider).
- all users should access approved online services using school-provided accounts (e.g. staff and students should register and login using a school provided email address).
- staff should have appropriate familiarity and a baseline technical knowledge.
- all members of the school community (students, teachers, parents) should understand that all school policies (e.g. Code of Behaviour, Acceptable Use, Anti-Bullying, Social Media, Safeguarding etc.) are equally applicable in a remote learning environment.
- where necessary school policies should have been adjusted or augmented to reflect remote engagement.
- essential transparency information should be provided to users (e.g. parents should have a clear understanding of how the school is connecting remotely with students).

The DES has published Guidance on Emergency Remote Teaching and Learning in a COVID-19 Context For post-primary schools and centres for education with advice applicable to situations where a partial or full school closure is necessary.

3. Real-time teaching and learning

Based on the experience of the past year, many schools have reached the view that with careful risk assessment and appropriate procedures in place, it is possible to deliver live streaming safely. Notwithstanding this, there have been some media reports about "lesson-bombing" where unknown third parties have joined an online class. We're aware of two different scenarios where this can happen, namely:

1. Pupils share the 'invite' to the class to an external person, who is then allowed into the virtual classroom by the teacher.
2. Pupils intentionally share their school login details with an external person, allowing them to freely gain access.

What might schools do?

- Ask your IT support providers to confirm that the settings on online lesson platforms ensure maximum security by default. The most secure systems will be those that only allow access to registered users.
- Remind teachers to pay attention to cases where a student appears to login twice (as an indication of another person using student credentials to join a class).
- Remind parents to check with children about the dangers of sharing information online, the risks involved and the fact that they are responsible for their behaviour online as they would be offline.

Teachers might also usefully revisit ground rules and expectations with students who are remote learning.

- Students might be reminded that facilitating a third party to enter an online class is a major contravention of the school's Code of Behaviour, with serious safety implications and potential consequences.
- Students may also need to be alerted to other implications. For example, after sharing passwords, students may find themselves locked out of their account and personal or sensitive information may be stolen, destroyed and misused.

JMB has produced an infographic on online classroom etiquette which may be helpful (also available as Gaeilge).

It might also be timely to remind students about the seriousness of taking screen grabs, recordings or photographs and sharing these, via social media or other means.

Ultimately, decisions on whether to use videoconferencing platforms in particular situations are for individual schools to make, based on whether it is perceived to be of educational value and whether it can be done safely. The JMB's Advisory note included substantial advice around the safe use of videoconferencing systems.

JMB has also produced an infographic summarising some recommendations about the safe use of Zoom for remote meetings and interviews.

4. Social Media Acceptable User Policy

An acceptable user policy (AUP) is a particularly important reference in terms of communicating the required standards of online behaviour and for helping to deal with any issues that arise. A school's AUP Policy may be generic (e.g. designed to cover all ICT-related activity for all members of the school community) or alternatively it may relate to a specific area of online activity (e.g. the use of social media) and a specific group of users.

Webwise, the *Irish Internet Safety Awareness Centre*, has an online AUP Generator which assists schools with customising an Acceptable Use Policy for pupils based on school needs.

A JMB template on Acceptable User Policy for Employees is available on the JMB website. It aims to assist employees in making ethical, respectful and acceptable decisions about their professional and personal social media usage and to provide clear direction on the importance of protecting the School's reputation and confidential information. For employees who are members of the School's teaching staff, the guidelines and AUP give effect to agreed professional protocols as prescribed by the Code of Professional Conduct for Teachers (Teaching Council, June 2012) which provides that teachers should:-

> *"ensure that any communication with pupils/students, colleagues, parents, school management and others is appropriate, including communication via electronic media, such as email, texting and social networking sites."*

5. Personal Data Breaches

Any security incident (such as Lesson-bombing or Screen-Grabbing) will need to be examined by school management to establish whether it necessitates lodging a report with an external body such as, An Gardai, the Data Protection Commission (DPC), and/or the school's insurance company. For example, in the event of a breach of personal data, the school is legally bound to file a report with DPC in circumstances where a potential risk has been identified.

The JMB Template on Handling a Personal Data Breach provides relevant guidance for school management. A related JMB webcast summaries the key advice around the use of this template. While any online security incident will present a concern, the level of risk will be significantly mitigated if little personal data was accessible (for example where the content being streamed was primarily curriculum-related rather than personal information, and with minimal sharing of device cameras).

For a fuller discussion of data protection issues, your attention is drawn to the JMB Template Data Protection Policy. The appropriateness of any school online activity should be considered in line with the guidance provided in the 7 data processing principles set out in Appendix 4 of this policy.
The JMB's Data Protection Advisor is available to discuss or advise on the above, or any other data protection issues. Please contact by telephone JMB 01 2838255 or email *cyrildrury@jmb.ie*

John Curtis
General Secretary JMB
9th February 2021