Appendix 4

ACCS Guidelines on the Use of Social Media in Schools

1. Introduction:

The internet and electronic communication have revolutionised the way we conduct business in schools and other organisations, and it is important to have policies/guidelines that help all stakeholders understand how they should use (and not use) these powerful tools.

At their best, these tools make us efficient, productive and better informed. Misuse, however, can create problems that distract from and undermine the school's mission. An effective social media policy/set of guidelines will encourage positive, productive communications while protecting an organisation/school from legal liability, reputational damage and security breaches.

- The policy/guidelines should be compatible with and form a part of the School AUP.
- Keep the policy/guidelines succinct and easy to follow.
- Review and update regularly.

Extract and adapted from https://www.focusdatasolutions.com/wp-content/uploads/2018/01/Effective-Email-Policy-Guidelines.pdf

Platforms

Advantages

- Connecting with stake holders in real time in relation to school information, e.g. meetings, important updates, deadlines etc.
- Celebrating student/teacher achievements, school/staff innovations
- Raising the school profile
- Efficient, fun and engaging manner of communication
- Can be used for Professional Development
- Increased local business engagement for student career development opportunities and potential sponsorship or events and venue hire income
- Improved internal communications among staff and students

Reasons to embrace the use of Social Media in Teaching & Learning

- **It is quickly becoming our duty as educators in the 21st century to guide our students towards responsible use of social media.** It is our duty to our students to start modelling responsible use of social media and encouraging them to follow our lead.
- **Social Media use is becoming our new first impression.** Many employers research the social networking sites of prospective employees. When our students start looking for jobs or applying for college, their use of social media is going to be studied. We need to ensure our students are portraying their skills and creativity in a positive way so that they can separate themselves from the pack and create opportunities for themselves that they may otherwise be shut out from.
- **Connected, community-based learning is important.** By blocking social media use, we are depriving our students of a huge opportunity to allow them to learn in connected ways. Society is moving toward a model of shared knowledge building, where people from all over the world can interact, question, reflect, and reshape thinking in meaningful ways.
- **Unfiltered Access.** Students have an unfiltered access point in their pocket, whether we want them to or not. We should be proactive in our efforts to guide our students towards responsible, productive use.

Schools addressing the use of Social Media are advised to access resources on:

https://www.webwise.ie/
https://pdst.ie/
https://www.pdsttechnologyineducation.ie
http://ppds.pdst.ie
http://schoolself-evaluation.ie/post-primary/

2. Steps to take when addressing the use of Social Media in schools.

1. Organise a Team

This could be a standalone team, or it could be a task allocated to an existing IT or Digital Learning Framework Team. This team should include teachers and non-teaching staff who use social media inside and outside the classroom and those who do not. School Management, Students & Parents should be represented also.

2. Examine Your School Culture

When setting out on this journey, it is important to understand the current beliefs about social media in your own school community.

Source information from all stakeholders.

- Examine how the use of Social Media can tie in with your school ethos and mission statement.
- Identify if, and how, Social Media is currently being used in your school.
- Outline how Social media can be used for the benefit of the school and for T&L.
- Define the role(s) of Social Media in the school.
- Assess risks in relation to the use of Social Media.

Some questions for reflection and sourcing information

- How are social media products currently being used by students? By teachers? By management and parents?
- How can they be used for better communication?
- What are the fears around social media in school?
- Is there a risk to individuals' right to privacy and right to have their personal data protected?
- Are there any "bright spots" where social media is already being used successfully?
- How can Social Media be used to benefit the school, student, teacher, parents, and management?

3. Establish a section in the AUP

This could cover the following:

- What are the goals in relation to the use of social media in our school?
- What platforms/Apps are used?
- Who has permission to post on school accounts?
- What type of content/pictures can be posted?
- Guidelines for student use of Social Media
- Guidelines for staff use of Social Media
  - Separate accounts for personal and school use
  - Timing in regard to the sending of emails
  - Procedures around teachers engaging with students on Social Media via:
- class or subject based accounts
- personal accounts
- Sanctions for misuse of Social media – students & staff

4. Establish a Timeframe for Review of Policy

As with all technology, Social Media is an area which changes quickly. Therefore, a Social Media Policy would need to be reviewed and updated on a regular basis.

3. Points to consider re use of/when developing a policy on use of emails in school

When exploring school culture, it may be useful to look specifically at practices in relation to communication in school and in this context, to review use of emails.

a. It should be clear, though it may seem obvious, that the use of a school email address is for school related purposes – that is, to conduct school business on behalf of the Board of Management in line with the employee's responsibilities. However occasionally a personal matter may be discussed via a business email account, so exceptions may apply and policies on how to handle personal email may be

practical and appropriate. *"…incidental and occasional brief personal use is permitted within reasonable limits, so long as it does not interfere with the employee's work."*

b. Following the principle of "business email is for business use," it is important to be clear that school email is the school's property.

There should be no expectation of privacy where school email is concerned, even if personal in nature. In other words, anything that is sent, received, created or stored on a company's computer system may be viewed.

Emails are part of the school's records and may be subject to discovery in a legal case.

The employer may monitor employees' use of email (it is legally important to make employees aware of potential monitoring).

c. What is NOT Allowed

In the interest of heading off bad or even illegal behaviour and protecting the school from liability, it is worthwhile to be explicit about what types of communications are prohibited by school policy. (AUP)

Effective Email Policy Guidelines

- may not be used to harass or make threats, nor be offensive or disruptive in nature;
- may not include language or images related to race, gender, age, sexual orientation; pornography, religious or political beliefs, national origin, or disability;
- may not present personal views as the school's own;
- may not engage in commercial activity unrelated to the school;
- may not distribute copyrighted material; and may not share confidential material, trade secrets, or proprietary information outside of the school;
- may not breach individuals' rights to privacy.

d. Receipt of Inappropriate Email

Employees should be encouraged to report the receipt of any inappropriate email with prohibited content to the ICT Co-ordinator or the Principal. The school should put a protocol in place to investigate and address any reports of inappropriate email in a timely manner.

e. Company and Network Security

Email may provide a window for security breaches and privacy and data protection breaches. Phishing and more specifically spear phishing emails have increased and are common cyberattacks on small businesses. Phishing refers to emails that appear to come from a legitimate source but are scams designed to steal private, sensitive information.

Some simple rules may include:

- Be suspicious of unknown links or requests sent through email or text message.
- Do not open email attachments from unknown sources, and only open attachments from known sources after confirming the sender.
- Never click on links in emails.
- Do not respond to requests for personal or sensitive information via email, even if the request appears to be from a trusted source.
- Verify the authenticity of requests from companies or individuals by contacting them directly.
- Any proprietary or sensitive information sent via email should be encrypted.

f. Retention

To the extent that a school has document retention policies, email policies should explain what should be retained, where and for how long. Check www.dataprotectionschools.ie for retention schedules.

g. Etiquette

Even if etiquette is not included as part of a formal policy, schools may wish to provide tips to employees related to:

- Professionalism – Emails should be professional and respectful in tone - err on the side of formal vs. casual.
- Spelling/grammar – Spell check should be enabled and grammar checked before sending emails.
- Proofread – Before sending, employees should re-read their emails to correct errors, check tone and avoid miscommunication.
- Address – Add the email recipient's address after composing the email to avoid sending an unfinished/unedited message. Double check the recipients' addresses before sending.

- Signature – Employees may be asked to include specific information as part of their signature (website address, phone number, social media links, or disclaimers).
- Reply all – To respect others' time and inbox capacity, limit replies to those who need to know the information being conveyed.
- Forward – It's probably best not to forward without permission, or at least to review all content that will be forwarded to avoid sending sensitive information. Do not alter others' text.
- Capitalisation – Avoid using ALL CAPS in email communications.
- Turnaround/response – Employees are expected to respond to emails both internally and externally within a reasonable (or set) timeframe.

h. Life Work Balance

Technology has dramatically improved the speed by which we can do business, but it can be abused. Depending on industry demands and a school's culture, it may make sense to set some parameters around email use to limit the intrusion technology can pose, both on personal lives and productivity. Schools may adopt policies that:

- limit the use of email after hours,
- limit email during holiday periods,
- limit the use of internal email (i.e. make colleagues talk to each other),
- limit use of email during certain work hours (dedicated "off-line" hours).

i. Availability of policy

To ensure that all stakeholders are aware of the school policy on email use, it needs to be readily available to them. The policy may be in the staff handbook, school journal and posted on the school website.

j. In Summary

Email is an important tool to facilitate communication and workplace efficiency. However, misuse can translate into legal trouble, reputational harm and security breaches. A thoughtful email policy tailored to your business can maximise email as a tool and avoid the undesirable consequences of poor judgement by any of the stakeholders. By setting clear guidelines about appropriate, ill-advised and unacceptable practice in relation to the use of email any organisation can gain peace of mind and a more productive workplace.

Source: https://www.focusdatasolutions.com/wp-content/uploads/2018/01/Effective-Email-Policy-Guidelines.pdf

4. Use of Apps in School – the importance of alerting parents/guardians to the general use of these in schools

An App 'APP' is an abbreviation of 'application'. An app typically refers to software used on a smartphone or mobile device such as the Android, iPhone, or iPad, as in "mobile app" or "iPhone app." These can be useful to enhance parent/guardian engagement in school life connecting parents/guardians to information about school events, calendars and policies.

The phrase "web app" or "online app" is also used to mean software that you access and use while online, via a browser, instead of software residing on your computer. Mobile apps have become very useful for schools by offering innovative ways to engage learners, help them study, and provide them with news and updates. The school uses apps for educational purposes, e.g. Kahoot and for informative purposes, e.g. School App used for announcements and keeping all stakeholders updated.

5. Establishing parameters around the establishment of and use of Instant Messaging Apps e.g. WhatsApp groups in school, by staff, PTA

ACCS recommends that particular care and consideration needs to be given to the use of Instant Messaging Apps by schools. Instant Messaging App groups are intended as a convenient way to distribute important school information to relevant people quickly and efficiently. These can be set up for a variety of reasons including by The Parents' Associations for example to allow people to communicate easily with each other regarding school matters. The person who sets up the group is the Administrator, Chairperson, Secretary, etc. It is vital to establish protocol and policy around the use of school WhatsApp groups which are set up to make lives easier.

Some Guidelines for good practice:

1. Always keep to the purpose of the group and do not use the group to discuss non-school related issues. Don't share irrelevant messages about other topics.

2. If your message is not relevant to majority of group members, please consider if it is more appropriate to reply by way of a personal message. Do keep the chat relevant to everyone and do not have one-on-one conversations in the group. Message the person directly instead.
3. Avoid in-depth conversations or arguments. Again, move this type of conversation outside of the Instant Messaging App group chat.
4. The Instant Messaging App group should not be used to post private or confidential messages or express personal opinions or gossip. Any opinions expressed are the opinions of individual members and may not be representative of the whole group. Group administrators are not responsible for any comments posted by individual members of the group.
5. Inappropriate posts include - posting promotions, using inappropriate language, personal attacks or insulting messages, bullying of any member, voicing grievances with the school or with individual members of the group. For individual concerns, please raise these directly with the parent concerned, teacher or, where necessary, the Principal.
6. It is not necessary to respond to every post unless it is requested e.g. RSVP, request for volunteers. If a message asks for a positive response, don't post a negative, e.g. attendance at an event, only post if you are able to attend. If a second request goes out about the same event don't reply twice.
7. If someone asks a question and you don't know the answer don't respond with "I don't know". Just wait for someone who knows the answer to reply.
8. Please respect the time you post. Agree times with the group which are not appropriate, e.g. early in the morning, late at night, at weekends and during school holidays etc.
9. By accepting a request to join the group participants agree to these group rules. Please note, by accepting the request to join, you are sharing your phone number with everyone in the group. Once you join, you always have the option to leave the group. Don't be offended if others leave. Not everyone wants the same information.
10. The group administrator has the right to restrict admission, remove or ban anyone from the group without any notification. Always seek permission before you add a person to a group. **Inform parents of the purpose of the group, seek permission etc. before adding students to any Instant Messaging App group.** When the group purpose is complete, delete it.

6. Points to consider when developing a social media policy for staff and students

Below are guidelines to follow when members of the school community (students and staff) are representing the school in social media spaces, regardless of whether these are considered professional or personal spaces.

a. Use good judgment

We expect good judgment in all situations. Behave in a way that will make you and others proud and reflect well on the school. Know and follow the school's Acceptable User Policy and Code of Behaviour. Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

b. Be respectful

Always treat others in a respectful, positive, and considerate manner.

c. Be responsible and ethical

Because you represent the school, please stick to discussing only those school-related matters that are within your area of responsibility.

Adults should be open about their affiliation with the school and the role/position they hold. If you are someone's peer, interact with them online if you are so inclined. If you are an employee thinking about interacting with a student, consider the following questions before proceeding.

- What is the purpose of my interaction with a student? (If it is not related to your classroom activities, reconsider using a social network.)
- What is the social network in which I propose to interact with a student? (If the social network in question has limited professional applications – Facebook, for instance – reconsider using that social network.)

If you are uncertain how to proceed, consult school management.

Share and interact in a way that will enhance your reputation, the reputation of others, and the reputation of the school, rather than damage them.

d. Be a good listener

Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly, and share feedback. Be responsive to others when conversing online. Provide answers, thank people for their comments, and ask for further feedback, etc.

e. Be accurate and appropriate

Check all work for correct use of grammar and spelling before posting. A significant part of the interaction on blogs, Twitter, Facebook, and other social networks involves passing on interesting content or sharing links to helpful resources. However, **never blindly repost a link without looking at the content first**.

And if you don't get it right ...

Be sure to correct any mistake you make immediately, and make it clear what you've done to fix the mistake. Apologise for the mistake if the situation warrants it. If it's a major mistake (e.g. exposing private information or reporting confidential information), please alert school management immediately so the school can take the proper steps to help minimise the impact it may have.

f. Be confidential

Do not publish, post, or release information that is considered confidential or private. Online "conversations" are never private. Use caution if asked to share your birth date, address, and mobile phone number on any website and never share the personal information of another individual without their permission

g. Respect private and personal information

To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal situations. Never share or transmit personal information of students, parents, staff, or colleagues online. While taking care when posting to safeguard people's privacy, be sure – as necessary and appropriate – to give proper credit to sources. In cases of doubt, privacy should be the default. Always respect the privacy of school community members.

h. Post images with care

Respect brand, trademark, copyright information and/or images of the school. Do not caption photos with the names of current students. Do not post photos of students who are on the "Do Not Photo" list. (Check with the relevant person on staff for details. (Such information will be captured in school application forms/school journals etc.) It is generally not acceptable to post pictures of students without the expressed written consent of their parents. Do not post pictures of others (colleagues, etc.) without their permission.

i. Be aware of site-specific guidelines

When posting images from school trips, do not post details (exact time and exact locations) of travel itineraries and plans. Post about the day's activities after the fact, avoid saying what you "will be" doing the next day.

j. Netiquette

Students should always use the Internet, network resources, and online sites in a courteous and respectful manner. Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet. Students should also remember **not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see**. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended. Students should not plagiarise ANY content from the Internet. Online research should always be cited and referenced.

k. Personal Safety

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

l. Students should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.

m. Students should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others.

n. **Cyberbullying** will not be tolerated. Harassing, impersonating, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary actions. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained by others.

o. Twitter

Many schools have main twitter accounts and other accounts from individual teachers and subject departments. It is important that teachers realise that when they tweet on behalf of the school, it should reflect well on the school. Teachers should be careful that the material they tweet/retweet is appropriate for all members of the school community and should only contain material that is school/subject related. Opinions should be avoided. Using a standard twitter handle (i.e. @AnywhereCS_subject) with a bio stating that it is an official account is advisable.

Examples of Acceptable Use

I will:

- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat social media carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Be cautious to protect the safety of myself and others.
- Be cautious to protect the privacy of myself and others.
- This is not intended to be an exhaustive list. Users should use their own good judgment when using social media.

Examples of Unacceptable Use

I will not:

- Use social media in a way that could be personally or physically harmful to myself or others.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Breach somebody else's privacy.
- Use language online that would be unacceptable in the classroom.
- This is not intended to be an exhaustive list. Users should use their own good judgment when using social media.

Source: https://www.sewickley.org/page/policies/social-media-policy

7. ACCS Template: SOCIAL MEDIA GUIDELINES & A.U.P. for staff

School Name

INTRODUCTION

These guidelines and A.U.P. have been developed to assist all employees of **[insert BoM, school details]** (hereinafter referred to as "the School") 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.

Social media refers to social and professional networking platforms such as Facebook, Twitter, WhatsApp, YouTube, LinkedIn, Snapchat, Instagram, blogs, message boards and forums and other similar online facilities.

The guidelines and A.U.P. are not intended to prevent employees from engaging in social media but are intended to inform employees as to what is considered by the School to constitute appropriate/inappropriate social media usage and conduct.

For those employees who are members of the School's teaching staff, the guidelines and A.U.P. 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."

and

"ensure that they do not knowingly access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or other format."

All employees should be mindful of what they post on social media, who can see it and how it can be linked back to the School and work colleagues. Misuse of social media can cause injury to others and can have a negative impact on the reputation of the School. Social media communications are never truly private and once information is published it becomes part of a permanent record.

Employees are **at all times prohibited from using or publishing information on social media which has the potential to negatively impact/reflect on the School and/or its employees and/or its students e.g.:**

- publishing defamatory, abusive or offensive material concerning any employee, volunteer, member of School management, parent(s), student(s), visitor or other member of the School community;
- publishing any confidential or sensitive information concerning the School or members of the School community;
- publishing material that might reasonably be considered to have the effect of damaging the reputation of the School.

The School reserves the right to take disciplinary action, up to and including dismissal, in respect of employees who engage in prohibited conduct and conduct in breach of this policy.

Given the ever developing and changing nature of social media and the internet the within guidelines and policy will be reviewed and adapted as required.

This policy should be read in conjunction with staff policies which are applicable to social media usage, in particular the dignity at work, internet and email usage, data protection, the Code of Professional Conduct for Teachers and other and disciplinary policies and procedures.

ACCEPTABLE USAGE POLICY

A. SOCIAL MEDIA USAGE ON A SOCIAL MEDIA SITE OR PROFILE ESTABLISHED IN THE COURSE OF EMPLOYMENT WHICH RELATES TO SCHOOL BUSINESS/MATTERS

(i) **Seek permission:** Employees must seek or have permission from the Principal/Deputy Principal(s) before setting up a site or profile relating to School business and or School matters/registering in the School's name on social media sites, user groups, special interest forums and bulletin boards/using social media for teaching and learning purposes.

(ii) **Property:** The property rights in a sanctioned social media account in the name of or on behalf of the School are vested in the School.

(iii) **Responsibility:** A permitted employee is responsible for his/her social media usage, for ensuring that private and confidential information is respected and protected at all times and for compliance with the terms and conditions of the relevant social media platform.

(iv) **Privacy & Confidential information:** Confidential information pertaining to the School, its employees, volunteers, students, parents and others in the School community must be respected and maintained at all times. Personal information about any students, parents, employees or volunteers must not be divulged or discussed on social media sites.

(v) **Unacceptable use:** Employees must not create, publish, download or communicate material/content that could reasonably be regarded as defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, damaging to the School's reputation or referring to a third person without their permission. Uploading, forwarding or linking to the aforementioned content is also unacceptable. Employees must never reveal sensitive details whether relating to the School, its employees, volunteers, students, parents and other members of the School community on social media sites.

(vi) **Behaviour:** Postings by an employee on a social media site that are defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, divulging personal data without consent or damaging to the School's reputation will be addressed pursuant to the School's disciplinary procedure and may result in disciplinary sanction up to and including dismissal.

B. PERSONAL SOCIAL MEDIA USAGE

(i) Boundaries: Personal profiles are not to be used to conduct school business or to communicate with students/parents. Online interaction with management, other employees and/or school contacts should be appropriate and professional in nature. Employees must not use the official School e-mail address when participating in personal social media/social media that is not related to the employee's job. Personal use of social media must not occur during working time but is restricted to break times at work.

(ii) **Identity:** Where an employee chooses to identify him/herself on social media as an employee of the School, s/he must make it clear that their communications do not represent the School, its ethos, position, opinions or views. The employee must write in the first person and state clearly s/he is posting in a personal capacity and not in the course of employment or on behalf of the School and state clearly that the views expressed are his/her own and not those of the School. Employees should at all times be mindful of their communications and possible consequences.

(iii) **Be mindful and respectful:** Employees must be mindful that their conduct not only reflects on themselves but also reflects on their professionalism and the School. Employees should exercise sound judgement, common sense and respect when participating in social media. Employees should not use insulting, offensive or disparaging language. If in doubt, don't publish or post anything. Information published online is permanent and never completely private.

(iv) **Responsibility:** Employees are personally responsible for their posts and actions on social media.

(v) **Privacy & Confidential information:** The obligations detailed at A(iv) above apply also to employees' personal social media usage. Do not divulge or discuss confidential information pertaining to the School, its employees, volunteers, students, parents and others in the School community and personal information, including photographs, of third persons (including employees, students, parents and other members of the School community) must not be posted, divulged or discussed without the permission of the person concerned.

(vi) **Unacceptable use:** Employees must not create, publish, download or communicate material/content that could reasonably be regarded as defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, damaging to the School's reputation or referring to a third person without their permission. Uploading, forwarding or linking to the aforementioned content is also unacceptable. Employees must never reveal sensitive details whether relating to the School, its employees, volunteers, students, parents and other members of the School community on social media sites.

(vii) **Behaviour:** Postings by an employee on a social media site that are defamatory, inappropriate, discriminatory, offensive, hostile, pornographic, divulging personal data without consent or bring the School into disrepute will be addressed pursuant to the School's disciplinary procedure and may result in disciplinary sanction up to and including dismissal.

REPORTING

Employees should immediately report to the Principal/Deputy Principal any inappropriate, abusive or defamatory or other unacceptable social media activity concerning the School, its employees, volunteers, students or other members of the School community. Such reports will be fully and confidentially investigated, the reported activity will be reviewed and, where appropriate, the content will be reported using the relevant online reporting mechanism.

ENFORCEMENT

The School will monitor social media usage on School computers, laptops, mobiles, tablets, notebook computers, smartphones, School accounts and School user names. The foregoing IT resources are the School's property and are to be used for legitimate School business. Whilst the School will not specifically monitor social media for references to the School, its employees, volunteers, students, parents and other members of the School community, employees should not expect privacy in this regard.

A reported or suspected breach of this policy is a serious matter and will be investigated by School management pursuant to the appropriate workplace procedure. The School reserves the right to use information that is expressly prohibited by this policy and which comes to School management's attention whether through monitoring or otherwise for disciplinary purposes.

Non-compliance by employees with any aspect of this policy may be subject to disciplinary action up to and including dismissal.

Dated, etc.

8. Establishing protocols re staff use of staff /personal devices when using for school business.

Staff may choose to use own device for school work or may use school device - an agreed set of ground rules/policy is important in either case. A formal policy not only helps protect the school, but it also alerts staff to their rights and responsibilities regarding school and personal information on the devices. Allowing staff to store and transmit school information on a personal device gives the school less control over information security. It is important for all stakeholders to be clear about their rights and responsibilities and terms and

conditions acceptable to the school and staff should be agreed in relation to these matters. Establish Acceptable Use Rules (AUP) and decide on the best way to review and update as necessary?

Areas to consider might include:

1. What is agreed in terms of who gets a school device? Are there parameters of use for school business/home use?
2. Will the school offer training on the device? Who is the go-to-person regarding training needs?

3. Who decides on which apps to use and what are the procedures if staff wish to set up online groups with students/parents/other colleagues?
4. Device maintenance and level of IT support school will provide for personal/school devices.

a. Staff responsibility for keeping the device updated.

b. Who should staff contact if they have questions about a device?

c. What level of support can the school provide/help fix a broken device?

d. Replacement policy re school devices?

5. How does a school ensure school information is secure - rules about device and file passwords and GDPR security? Is there clarity about backing up school information/data and to where? What are the expectations about copying, storing and backing up sensitive data/information?
6. Mobile devices allow for greater risk of theft and loss and virus compromising the system. Is there a clear procedure for staff to follow in the event of any one of these happening? To whom should staff report (timeframe) and is there a procedure in place to delete/wipe the device of all data? Personal data may be lost and staff should be aware of this. This should tie in with the school Data Breach notification Procedure.
7. What procedure is in place regarding the monitoring of the use of and the information on the devices? Have you considered whether permission is required from individuals before monitoring information on the device? Will personal data be contained on the device?
8. What is agreed in terms of departure procedures when staff go on leave of absence, quit, retire etc.? How is the information on the device which is school related and owned by the school secured?

9. External Speakers

Ref Circular No. 0043/2018

Best practice guidance for post-primary schools in the use of programmes and/or external facilitators in promoting wellbeing consistent with the Department of Education and Skills' Wellbeing Policy Statement and Framework for Practice.

School management, principals and teachers have a duty to provide the best quality and the most appropriate education in order to promote the wellbeing of their students. They also have a duty to protect students in their care at all times from any potentially harmful, inappropriate or misguided resources, interventions or programmes.

This circular offers best practice guidance in selecting wellbeing promotion programmes and/or external facilitators (both once-off speakers and those delivering programmes over a period of time), to support the implementation of the Wellbeing Promotion Process including, in particular, the selection for social, personal and health education (SPHE), and relationships and sexuality education (RSE) curricula.

All visitors to the school including guest speakers, while not employees of the BOM, are subject to the school AUP guidelines. Schools may choose to keep control of Wi-Fi codes and issue a guest code to visitors which expires within a working day/a number of hours. Generally, the guest code is made available at school reception with the reminder that all guests are subject to the school AUP guidelines.