

Remote/Off-Site Working Advice for Schools

Education Hub / Department for Education (DFE)

Recently, the DFE have published an advice document to promote the importance of safe working practice and Cyber Security whilst working remote/off-site during the COVID-19 Pandemic. This is to provide school staff with clear advice for addressing and minimising potential threats to Cyber Security and Data Privacy.

We are already doing such a great job at staying safe whilst working from home and already doing most of these things listed below. This document is a reminder to ensure that we know how to remain safe and secure whilst working remotely.

Below I have summarised key points from the document, which are relevant to us at St John's:

1. School Policy and Procedures

- Staff should remain conscious of the school's reputation when using communication platforms such as emails. Even though we are working in a home environment, professional standards still apply.
- Please keep your school laptop to yourself, especially when connected to the remote server, and do not lend your laptop to anybody including children.

2. Cybersecurity

- Staff must report malware/ransomware /data breaches/ security issues immediately.
- Staff should lock screens when leaving their laptop unattended.

3. Passwords

- *Do not share your password with others; passwords are the first line of defence for your computer system.*

4. Phishing Emails & Scams

- Phishing scams are designed to look like legitimate messages to trick the email recipient into providing information or clicking on a bad link. The police have reported a significant rise in phishing scams. Therefore, be extra vigilant for possible malicious activity and only open emails from trusted recipients.
- Staff must report malware/ransomware infections immediately.
- Be cautious about pop-ups about virus warnings when accessing the Internet. Be wary too, of messages reporting to have detected a virus when this is not reported by the school.

5. Online Meetings & Video Conferences

- In the current situation, *we are using Microsoft teams for online meetings and conferences.*
- It is important for you to know how to block (or pause) the webcam if you do not want to be seen in the meeting.
- When appearing on camera, be aware of what may be visible in the background of the picture and dress appropriately.
- Do not have confidential calls and discussions near other members of the household and be aware that smart speakers like Amazon's Alexa, Apple's Homepod and Google's Home may record limited data and should be avoided when undertaking sensitive calls.
- Muting microphones when staff are not speaking in a conference call minimises the impact of background, household noise. Use headsets if available.
- Meeting and conferences should not be recorded, unless this feature is desired. If recording is the intention, attendees need to be aware and permission needs to be sought.

6. Data Protection

- Staff should not provide private contact details and should only use work email addresses to contact the wider school community e.g. parents.
- Do not use USB flash drives and cloud services to store personal or school data.
- It is our responsibility to respect the privacy of pupils and other staff therefore do not breach confidentiality.
- Data breaches, such as sending emails to wrong recipients, must be reported and recorded to meet with the GDPR. Staff should advise as soon as they become aware of any possible breach.

More information can be found at:

<https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19>