

 **Remote or Off-site Working**

 Updated September 2021

Version 2.0

**Contents**

[**The aim of this document 3**](#_Toc83386291)

[**The purpose of this document 3**](#_Toc83386292)

[**Audience 3**](#_Toc83386293)

[**Introduction 3**](#_Toc83386294)

[**1. School Policy and Procedures 3**](#_Toc83386295)

[**2. Cybersecurity 4**](#_Toc83386296)

[**3. Passwords 4**](#_Toc83386297)

[**4. Phishing Emails & Scams 5**](#_Toc83386298)

[**5. Online Meetings & Video Conferences 5**](#_Toc83386299)

[**6. Data Protection 6**](#_Toc83386300)

[**7. Backup 7**](#_Toc83386301)

[**8. Reporting Harmful Content 7**](#_Toc83386302)

# **The aim of this document**

To promote the importance of safe working practice and cyber security for remote/off-site workers.

# **The purpose of this document**

To provide school staff with clear advice for addressing and minimising potential threats to cyber security and data privacy.

# **Audience**

This document is intended for Headteachers, Business Managers, IT Managers, and IT Co-ordinators.

# **Introduction**

Cyber-crime is on the increase and simple measures can drastically reduce the likelihood and effects of cyber-attacks. As well as cost implications, physical impact, and reputational damage, cyber security breaches can also lead to unauthorised access to information of a sensitive nature. All school staff need to be up to date on the latest cyber security threats and the best methods for protecting data.

Mobile devices are now **critical** to the functioning of your school. It is vital staff follow school policies for software-updating, backups, and protective-controls such as strong passwords and encryption.

# **School Policy and Procedures**

Whilst school staff are working remotely, they should still follow school policies and understand their responsibilities relating to confidentiality and security. School policies and procedures protect both individual staff and the school, enabling the school to maintain functions and provide the structure needed to continue to provide services to children and families.

1.1 Take this opportunity to remind users about your Acceptable Usage Policy (AUP). Remind staff not to lend their machines to their children or other members of their family.

1.2 Staff must be conscious of the school’s reputation when using communication platforms. Remind staff that professional standards apply.

1.3 Keep a printed copy of your procedures and checklists offsite, or securely store them in the cloud.

1.4 Remind staff that you can monitor/check their activity as per your policies and terms and conditions of employment. At home, staff may 'forget' they are using work devices and the delineation is more blurred.

1.5 Have a designated method for staff to send critical messages (health, safety, mental health, security incident) quickly and securely. Consider how this would work if the issue was IT related.

1.6 If using file sharing services be sure to check who has 'modify or read-write' access, who can view and who is the document owner. Ensure there is access to school policies and key documents for staff.

# **Cybersecurity**

Your school network is the lifeline of your school whilst staff are working remotely/off-site and it is necessary for staff to take steps to protect your systems and your data. Schools are advised to consider who in their institution has the technical knowledge to maintain safe IT arrangements, and what their contingency arrangements would be if their IT staff become unavailable.

2.1 Staff must report malware / ransomware / data breaches / security issues immediately and should be advised how to do this.

2.2 Ensure you review/audit permissions and privileges for systems and that any new requests for access go through a central point, rather than to a provider directly.

2.3 Ask staff to keep all their devices fully updated and not to defer updates.

2.4 Remind staff to lock screens when leaving their machines unattended.

2.5 All mobile devices must have full disk encryption.

2.6 If you are loaning laptops/desktops to staff, ensure they are reset and checked upon return. This must be on top of your to-do-list when things go back to ‘normal’.

2.7 Most school devices are restricted from downloading apps, but remind staff using their own devices not to download apps from non-trusted sources. Malware is more common in a crisis situation.

2.8 Filtering and monitoring is still an essential part of provision and is needed to meet with safeguarding requirements laid out in the [Prevent Duty](https://www.gov.uk/government/publications/prevent-duty-guidance).

Filtering can be tested by using the SWGfL tool, which is available here: <http://testfiltering.com/> with full [Guidance on filtering](https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering) available from the UK Safer Internet Centre.

2.9 Schools are advised to undertake an online safety review, such as using the 360o Safe Tool. <http://www.360safe.org.uk/>

# **Passwords**

Passwords are the first line of defence for your computer system. Passwords are used to verify identity and confirm access rights, and system security relies on these. Make sure your staff have access to all the systems they need and that they are able to access relevant accounts. Timeouts are likely to be more common where staff are not logging on to school systems as regularly.

3.1 Staff must not share passwords or share user accounts.

3.2 Advise staff to use password managers (Using a very strong password for the password vault) if they have a high number of passwords to remember.

3.3 Ensure you have reset procedure in place for password timeouts or in case passwords are forgotten.

3.4 Password protected documents should be sent with another form of communicating the password, such as a telephone call.

3.5 Staff using personal devices for schoolwork should ensure they follow school guidance on password complexity.

3.6 Passwords containing three random words together are recommended for security.

# **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. Most of these allege to be news articles and updates about coronavirus. Systems for collecting information from schools will use secure methods, communicated to school leaders in advance.

4.1 Remind staff not to open links or documents with coronavirus information unless they are sure of the source.

4.2 Remind staff that critical emails will only come from specific email accounts and advise them of trusted addresses.

4.3 Be vigilant for possible malicious activity on user accounts and ensure prompt reporting occurs if emails are getting swamped with SPAM. This is especially important if the source is another staff account.

4.4 Remind staff that it’s ok to make a mistake and that they should own up if they have accidentally clicked on a suspicious file and or link.

4.5 Staff must report malware/ransomware infections immediately.

4.6 Remind staff to 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 installed and recognised anti-virus software. Certainly, no genuine software would ask for money to 'clean up' a virus. This is malware.

# **Online Meetings & Video Conferences**

In the current situation a number of schools want to use conferencing software. Microsoft Teams is available to schools through their existing Microsoft Office licenses. Any chosen system should be subject to the usual due diligence around data protection and information security.

A DPIA screening for Microsoft Teams and Zoom is available via Derbyshire’s [SchoolsNet](https://schoolsnet.derbyshire.gov.uk/administration-services-and-support/coronavirus-information/information-and-advice-to-schools.aspx)

5.1 Advise staff of the preferred / approved conference app and ensure all staff know how to use the chosen platform.

5.2 The chosen platform may need to be subject to Data Protection and Security checks. These should be documented, where appropriate.

5.3 Ensure staff use basic security and privacy settings such as having a password to join a meeting or conference call, blocking cameras by default to allow the user to be shown when ready, and knowledge of how to remove themselves or others from a meeting.

5.4 Remind staff not to have confidential calls and discussions near other members of the household. Smart Speakers like Amazon’s Alexa, Apple’s HomePod and Google’s Home may record limited data and should be avoided when undertaking highly sensitive calls.

5.5 Muting microphones when staff are not speaking in a conference call minimises the impact of background, household noise. Use headsets if available.

5.6 Educate all staff to ensure webcams are blocked by default so that users can enable only when they are ready to have their image displayed. Be aware of what may be visible in the background and dress appropriately.

5.7 Meeting: State that meetings should not be recorded, unless this is feature is desired. If recording is the intention, permission from attendees needs to be sought.

5.8 Lessons: State that lessons/tuition should not be recorded.

5.9 Remind staff to EXIT or close the app once the conference is complete.

# **Data Protection**

Data Protection may be more of a challenge with sudden changes in working practice and the need to implement systems at short notice. Data Protection rules will not stop you doing this, but protecting personal data is still essential. Whilst some staff may be working from home, others may be providing childcare within the setting. Safeguarding is still the highest priority and concerns surrounding the welfare of an individual should be communicated promptly.

6.1 Remind all staff of their responsibility to respect the privacy of pupils and other staff and maintain confidentiality. Schools asked for a list of vulnerable children or similar for charity donations must not give out personal information. Ask parents to contact the school to 'opt-in' for any services offered.

6.2 Staff should not provide private contact details and should only use work email addresses to contact the wider school community.

6.3 Staff should not store personal information in non-approved locations. There should be no data stored on the hard drive of any machine, remind staff of this.

6.4 Remind staff they must not use unapproved USB flash drives and unapproved cloud services and that data protection is their individual responsibility.

6.5 Ensure that any documents removed from site are signed out by the individual with an additional approval signature from a designated person.

6.6 Ensure strong security surrounds any documents removed from the school site and that files are locked away. Ask staff not to print personal information unless the communication are intended to be sent as a hardcopy.

6.7 Staff should be reminded to encrypt personal information sent via email.

6.8 Staff must advise senior leaders of any new service or solution that they want to use. New systems need to be subject to the same due diligence and DPIAs should still be signed off by the DPO and Governors.

6.9 Remind staff that 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 without fearing repercussions.

# **Backup**

Backups are critical for ensuring that the school can keep providing services in the event of damage to the network, outside attack or accidental data loss. It is important school backups run regularly and that it is checked to make sure the backup successfully contains your files.

7.1 Ensure staff save their critical documents to the server or to a school approved cloud storage, such as OneDrive or Google Drive.

7.2 School backups should be run regularly and verified as complete. If encrypted USBs / removable drives are permitted, these need to be backed up manually by the individual staff member.

7.3 Ensure you have a robust Cyber Incident Plan in case of attack and know who is responsible for each identified task.

7.4 Cloud providers like Google and Microsoft are responsible for the availability of their Platform - schools/users are responsible for backing up their actual data.

7.5 GSuite / Office365 does not offer the same eDiscovery & advanced search functionality as dedicated backup products. Ensure you don’t rely on cloud storage as a backup solution.

# **Reporting Harmful Content**

It is important that staff and pupils report any harmful content or any concerns via one of the following:

UK Safer Internet Centre - <https://reportharmfulcontent.com/>

CEOP - <https://www.ceop.police.uk/safety-centre/>

Criminal activity / cyber-crime should be reported to [Action Fraud](https://www.actionfraud.police.uk/) online or by calling **0300 123 2040**