PROTECTING YOUR PRIVACY ONLINE

Contents

Wireless networks have transformed the way we are able to use computers and mobile devices, in the home, workplace and when we are out and about, offering flexibility to communicate with others, to access information, to process data and make transactions at any time.

Computers and many other devices, including tablets (e.g. iPad), laptops and smartphones, can connect to the internet wirelessly using Wi-Fi. Home and office wireless networks make it easier to use the internet and send and receive e-mail in any room in the building and even outside. Public wireless networks or hotspots also enable individuals to do their work anywhere, including places like cafés, hotels and even on the street. Plug-in mobile broadband devices provide even more flexibility, allowing individuals to work online where there is cellular 3G or 4G coverage.

However, there are important issues regarding your privacy and security that members need to consider when using Wi-Fi and when receiving, storing or transmitting data or information online.

The security risk associated with using any system which is internet based or which accesses the internet is that unauthorised people may be able to intercept what you are doing online. This could include capturing your passwords and reading your private and confidential material.
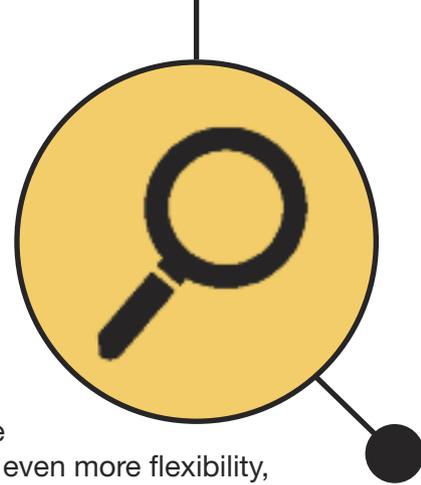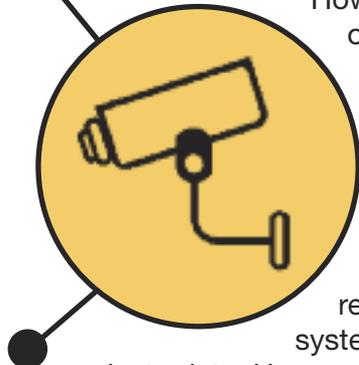
Privacy

Maintaining privacy whilst online is essential for avoiding the theft of your identity or personal records, and to prevent fraudulent behaviour.

However, it is surprisingly easy to inadvertently give away your personal information online without knowing that you have done so. This can have serious implications for you, including identity theft, financial loss, defamation, blackmail or extortion.

Many schools/colleges use IT systems for storing personnel and pupil records. Many of these systems will include personal and sensitive information about individuals. Some employers, for example, are using cloud-based IT solutions to store and provide access to payroll information, including to provide staff with pay notices at the end of each month. Schools/colleges (i.e. 'data controllers') are responsible for ensuring the safe and secure management of such data via any IT systems they use and are also responsible for ensuring the security of personal and private data. However, members should also be clear about what information about them is stored or transmitted online and act appropriately to ensure that the security and privacy of personal and sensitive information about yourself or others is not compromised.

The Importance of Privacy

The General Data Protection Regulation (GDPR) provides for a legal framework of responsibilities on organisations (including schools and colleges) and employers, and rights for individuals (including teachers) with regard to ensuring privacy and confidentiality.

The GDPR requires organisations to process personal data fairly and lawfully, based on eight principles (see Annex), in order to protect the interests of individuals whose personal data is being processed.

Schools, colleges and other organisations are defined under the GDPR as 'data controllers' and are thereby responsible for ensuring the security and integrity of personal data that they hold or process. The GDPR imposes a duty on schools and colleges to take appropriate steps to prevent the unauthorised or unlawful processing of personal data and to safeguard against the accidental loss or destruction of, or damage to, personal data. Regardless of the arrangements or method for the storage, processing or transmission of personal data, the school/college, as the data controller, is responsible for compliance with the provisions of the GDPR.

Your Shared Responsibility

Members should recognise their responsibility to avoid inadvertently communicating, transferring, deleting or posting personal data about others online.

Individuals could be in breach of the law when posting online if they post information which subjects others to harassment or abuse. Individuals can be prosecuted through the criminal courts and could be sued for damages in a civil court. In a non-personal capacity, where a person is representing an organisation (e.g. a school, college or trade union), both the individual and their organisation should comply with the GDPR data protection principles.
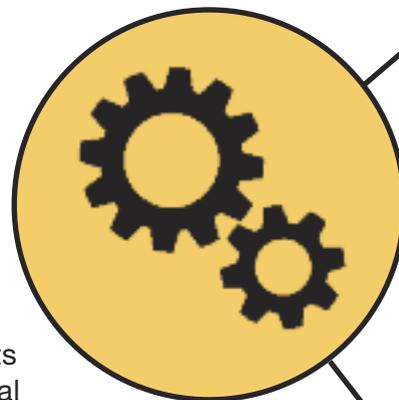
Data Protection Risks
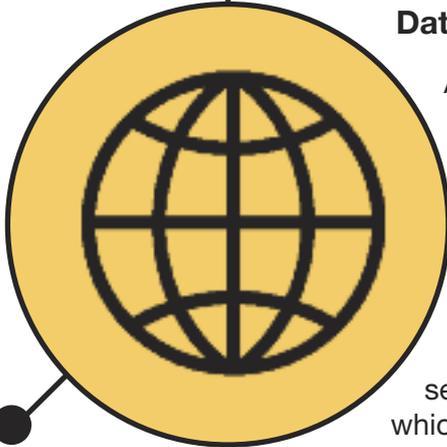
Advances in technology have enabled organisations to process more and more personal data, and to share information more easily. Whilst this has many advantages, it also gives rise to increased security risks. Put simply, the more databases that are set up and the more information that is exchanged, the greater the risk that some data will be lost, corrupted or misused.

Whenever information is stored or disseminated using IT-based systems and online networks, there will be a risk to privacy and data security. The security risk associated with using any system which is internet based or which accesses the internet is that unauthorised people may be able to intercept what you are doing online. This could include capturing individual passwords and reading private and confidential material without authorisation.

Home and school/college wireless networks make it easier to use the internet and send and receive e-mail. Public wireless networks or hotspots also enable individuals to do their work anywhere. However, consideration should be given when using wireless networks which may make it easier for hackers to access private files and information or allow others to access your home or school/college internet connection in ways that could be detrimental to you personally or professionally.

In some cases, links to bogus websites sent via e-mail or through social media accounts such as via Facebook or Twitter may also be used to access personal, private and sensitive information. Some scammers also use telephone calls to ask individuals to confirm information about themselves as a pretext to fraudulent and criminal behaviour.

It is the responsibility of the school/college to ensure that it has systems in place to ensure the security of all of the personal data it collects and holds, regardless of where information is stored – e.g. on a server or saved on a memory stick. As a minimum, the data controller (school/college) should ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority;
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

If a breach of security occurs, the school/college has a responsibility to report the breach to the Information Commissioner's Office.

Where an individual suspects that there has been a breach to data security (whether to their own or someone else's personal data), this should be reported as a matter of urgency to the person responsible for data protection matters.

NASUWT members should contact the Union immediately if they believe that their own personal data has been compromised.

Working from Home

Members who choose to work at home should recognise that it is their responsibility to obtain permission from their employer before processing or simply holding personal data at home, including personal and sensitive data relating to individual staff or pupils. This is important where files containing such data are taken out of the workplace (e.g. on a memory card/stick) or accessed online, regardless of whether you intend to access or use any data that may be personal or sensitive.

Members will need to take sufficient precautions to ensure that personal data about staff or pupils cannot be accessed by any unauthorised third party, including family members, friends or others. Files should always be password protected, and steps should also be taken to use secure devices including computer/device, secure Wi-Fi and media storage (e.g. memory cards, USB memory sticks).

Swapping data storage devices such as memory cards between work or home computers and devices may also compromise security of the school/college IT systems and your own personal system, particularly if data devices contain malware or viruses which could harvest or destroy data. It is important to remember that loss of data is also an offence under the GDPR. A data controller (school/college) and data user (teacher) would be expected to explain the circumstances for any loss and demonstrate that taking data off site was justified and that the risks associated with doing so had been managed appropriately.

Using your own IT Equipment

Members should avoid using their own IT equipment/devices (including computers, tablets, smartphones and memory cards), whether in the workplace or elsewhere, for work-related purposes, without the written agreement of the employer. Where members are required to use IT equipment for work purposes, the equipment/devices should be provided by the employer. It is important that any devices provided by the employer are used solely in accordance with the provisions of the employer's Acceptable Use Policy, and should not be used for your own personal purposes.

It is important to keep work-related devices and systems separate from devices used for personal/private purposes at all times. This means, for example, ensuring that you have discrete/dedicated computers/devices for your own personal online activity.

Whilst using personal IT equipment may be permitted within an employer's Acceptable Use Policy, a school/college will need to ensure that the devices an individual intends to use will not compromise data security within the school/college. This may, therefore, require an employer to monitor and check the use of an individual employee's own computer or devices to ensure compliance with the Acceptable Use Policy. This may have implications for the privacy of any data, materials or online history that could be identified from an individual's use of their own computers/devices.

Unsecured Wi-Fi

The main security risk associated with using your own device in a public place is that the Wi-Fi may not be secured, enabling unauthorised people to intercept anything you are doing online. This could include capturing your passwords or your private and confidential documents/materials. Unsecured Wi-Fi also risks compromising your identity, including your financial or banking details. A risk to an individual's privacy and security can happen if the connection between their computer or smartphone and the Wi-Fi signal is not encrypted, or if someone creates a bogus hotspot which purports to be legitimate.

Where unsecured Wi-Fi is used in the course of day-to-day work, this also has the potential to put at risk the school/college's data security.

Cloud Storage

Some schools/colleges are migrating their IT systems from physical data storage systems to online or cloud storage solutions. Cloud storage refers to the storage of data on online platforms controlled by another organisation. These solutions are often used by organisations to save costs associated with data storage, or to improve accessibility to data, or to back up data to safeguard against the loss of data. However, cloud storage carries risks which have implications for individual teachers.

There is no such thing as a completely safe cloud system. Whenever data is stored on the internet, it is at risk of a cyberattack or being 'hacked', particularly if data is not encrypted, or where the means of accessing the system (e.g. a computer or a network) is not secure.

The scale of impact of a data security breach may also be multiplied where data is stored in the cloud. If the security of a cloud platform is breached, then all of the data stored may potentially be compromised or lost. Access to data stored in the cloud may also be affected if an online server fails or cannot be accessed for any reason. This can have serious implications for managing day-to-day school/college systems and processes.

The third-party provider, not the school/college, controls the maintenance and security of the data stored in the cloud system. This means that a third party, in essence, has access to an individual's personal data, creating an added layer of risk for data security and privacy.

Schools and colleges should therefore consider carefully what data would benefit from cloud storage. Cloud storage may not be a solution for all forms of data, especially if the risks associated with the use of such solutions cannot effectively be managed.

Schools and colleges should also consider that cloud storage providers may wish to process the personal data stored for their own direct marketing purposes. This is a matter for the school/college as data controller to agree or not. However, individuals whose data is kept by a cloud storage provider must be given the right to prevent their personal data being used for direct marketing. Schools and colleges have a duty to explain to staff, parents and/or pupils what personal data will be held about them, how it will be collected and stored, how it will be used and by whom, and what rights they have over the use of their personal data.

The school/college should ensure that it exercises due diligence in the selection of a cloud service provider in order to meet their duty under the GDPR.

Social Networking

Online social networking is now a part of everyday life for many teachers. Various social networking sites are also valuable tools used by many teachers, and are encouraged by some employers and professional development bodies. However, using social networking sites carries a degree of risk to privacy and security.

Whether social networking platforms and forums such as Facebook, Twitter, TES, LinkedIn and others are used just to contact other people, share information, post photographs of an important meeting, event or a holiday, it is likely that this will include the exchange of at least some personal information about yourself or others which could pose a risk to your privacy or even your personal safety.
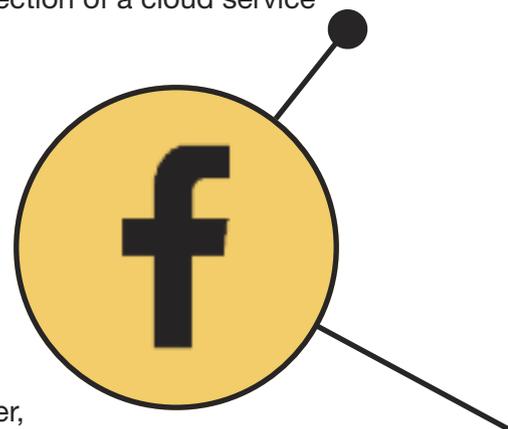
Most social networking sites allow users to apply privacy settings to control how public or private the information that they post online will be. Before posting information or images on social networking sites:

- check the privacy settings and adjust them to ensure you do not risk sharing information about yourself or others (e.g. your family or colleagues) with people you do not want to;

- review your privacy settings regularly;

- bear in mind that on some social networking sites, people that are not your approved 'friends' will still be able to see some of the information you post online;

- use strong passwords and logins to prevent unauthorised access to your social networking account and privacy settings;

- choose a user name that does not include any personal information;

- avoid posting personal information about yourself – either in your profile or in your posts (e.g. telephone numbers, pictures of your home, workplace or school, home address, birthday, holiday plans) – that could make you vulnerable to identity fraud, theft or harm;

- think carefully before posting information which other people might be able to access and use against you – for example, your employer or a potential employer, or a colleague, parent or pupil;

- obtain consent from other people (especially colleagues, parents and pupils) before uploading their pictures or personal information;

- have separate social networking accounts for your work and personal activity online;

- beware of 'phishing' scams, including fake 'friend' requests and posts from individuals or organisations inviting you to visit other pages or sites;

- ensure you have effective and updated antivirus/antispyware software and a firewall running before you go online.

Ensuring Privacy Online ————●

Ensure you always have effective and updated antivirus/antispyware software running on your computer.

Only use secure Wi-Fi networks and ensure your home network is also secured.

Do not leave your computer, smartphone or tablet unattended in public places.

If you are using your computer, smartphone or tablet in a public place, be aware that there will be other people around you who may be watching what you are doing online.

Unless you are using a secure web page, do not send or receive private information when using public Wi-Fi.

Only use secure websites when making transactions online, including when banking online, checking personal information records, or when reviewing any private, sensitive or confidential information online.

Always log out of secure websites as soon as you have completed a transaction and before you log out or turn off your computer/device. Closing the window or shutting down your computer may not automatically log you out of the website you have visited and may make your information accessible to someone else who might be using the same computer/device.

Always use strong passwords (a mixture of lower and upper case letters and numbers) and change your passwords regularly. You should never reveal your password to anyone else.

Keep passwords and Wi-Fi codes safe so that others cannot access or use them.

Check what data is stored about you, including data about you using cloud storage. Find out about what controls are in place to ensure the security and integrity of data about you.

Check whether information held about you might be used for direct marketing purposes. If you have any concerns, you have the right to stop your information being harvested or passed to other organisations for the purpose of direct marketing.

Use search engines (e.g. Google, Bing) to check for any information that may have been posted online about you. Contact the author, website administrator or search engine provider to have any inaccurate or malicious information removed.

Do not use a work e-mail address for personal use. It is far better to have a separate, private e-mail address for private use. Where personal information is transmitted using a work e-mail address or using a computer/device or network provided by your employer, it may be accessed by your employer at any time.

Use any computers/devices provided to you by your employer solely in accordance with the provisions of the employer's Acceptable Use Policy, and not for your own personal purposes.

Keep work-related devices and systems separate from devices used for personal/private purposes at all times.

Avoid swapping data storage peripherals between work and personal computers/devices, especially without undertaking appropriate antivirus checking.

Do not access links to unknown or bogus websites or open e-mails from unknown or suspicious sources.

Do not provide personal or private information in response to unsolicited telephone calls.

Check privacy settings and adjust them to ensure you do not risk sharing information about yourself or others (e.g. your family or colleagues) with people you do not want to.

Do not use unsecured Wi-Fi networks whether in your home, office or when out and about.

Ensure your wireless hub/router is secured so that other people cannot easily gain access to sensitive information that you may be sending or receiving online. This is an important precaution when you are working and using your own equipment to communicate online. Simply search for available wireless networks, and those that are secured will be indicated with a padlock symbol.

Check that your device does not auto-connect to Wi-Fi signals. If your device is set to automatically connect to available open Wi-Fi networks, then you run the risk of automatically connecting to unknown and potentially dangerous networks. You should switch off auto-connect via the device settings page.

Other Support for NASUWT Members ———————●

The NASUWT recognises that computers and devices such as tablets (e.g. iPads) and smartphones are helpful in enabling individuals and organisations to communicate, stay in touch and share information. In an employment context, teachers can often benefit from the advantages of being able to manage their work in ways and at times that suit them. However, there is also the danger that such flexibility has the potential for increasing workload and for unrealistic and unreasonable demands to be placed upon individuals.

The NASUWT is the only union that is pursuing industrial action to protect teachers and headteachers from excessive workload associated with using e-mail and other online communication systems.

For more information about the NASUWT industrial action, go to: www.nasuwt.org.uk/IndustrialAction.

Wherever members encounter any issues or have concerns about the use of personal data, they should contact the NASUWT for help and advice.

E-mail: advice@mail.nasuwt.org.uk
Tel: 03330 145550

ANNEX 1

General Data Protection Regulation – Rights for Individuals

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

For more information on what these rights mean, please go to www.ico.org.uk.

ANNEX 2

TIPS FOR MANAGING DATA SECURITY

1   **MANAGE YOUR PASSWORDS:**
Ensure your passwords are strong, changed regularly and are not shared or written down.

2   **LOCK IT UP:**
If your device is left unattended, make sure that it is locked so that others cannot access it.

3   **PROTECT MOBILE DATA:**
If you use USBs or other flash drives, password protect them.

4   **WATCH OUT FOR MALWARE:**
Think about what you plug into your computer. Malware can be found on infected flash drives, external hard drives and even smartphones. Please contact your IT department if you suspect that you have been the victim of malware.

5   **TAKE CARE WHEN SHARING DATA:**
Have clear, safe systems for sharing data and share safely. Do not send lists of personal data on e-mail without password protection. Do not send lists of personal data via the postal system.

6   **BACK UP YOUR DEVICE:**
Back up regularly and make sure that you turn on AutoSave.

7   **BE SAFE ON THE INTERNET:**
Ignore unsolicited e-mails, be wary of attachments and links from people you do not know and avoid unnecessary downloads.

8   **PHYSICAL DATA MATTERS TOO:**
Do not leave personal data on your desk when it is unattended. Lock away personal data at the end of the day.

9   **SHRED WHAT YOU DON'T NEED:**
Shred any physical personal data you no longer need straightaway.

10   **REPORT ANY DATA BREACHES:**
The Information Commissioner states that a personal data breach is: 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service'.