Digital Skills for Heritage:

Online Privacy and Security

Produced by Naomi Korn Associates
for The National Lottery Heritage Fund

HERITAGE FUND

naomi korn ASSOCIATES

Digital Skills for Heritage

Introduction

Heritage organisations find themselves working increasingly online, and the coronavirus (COVID-19) pandemic has made this more necessary than ever before. Safeguarding the privacy of people in and across the heritage sector, and keeping information secure, are particularly important as we adapt to new ways of working remotely.

This guide looks at some of the online activities carried out by UK heritage organisations, and addresses a range of issues they are likely to encounter. It includes checklists, practical advice and resources to help understand and manage online activity. Use this guide according to the needs of your organisation to help you, and the communities you support, stay safe.

Online privacy and security

Staff and volunteers working across the heritage sector support and connect with a diverse range of communities. We collect, preserve and provide access to a range of objects, buildings and spaces. We also produce information, resources and activities, including digital resources and activities that take place online. Making use of technology enables us to:

- work from home and at distance
- communicate and collaborate with co-workers and volunteers
- engage with audiences and answer questions
- keep in touch with members and patrons
- provide access to resources and buildings

> **Although data protection laws don't apply to people who are no longer alive, there will still be a surprising amount of personal data in your collections management system and you need to keep it safe. Being aware of what personal data you do hold – cybersecurity, password protection and so on – are all crucial.**
>
> Gordon McKenna,
> Standards Manager,
> Collections Trust

Privacy and data regulations

Heritage organisations must comply with a range of legal responsibilities in this online space. Whether board member, employee or volunteer, we all have a responsibility to make sure we comply with the security, data protection and privacy policies in our organisations. These policies explain how the legal responsibilities relating to the security of personal data and acceptable online behaviour are managed. The Data Protection Act 2018 incorporating the General Data Protection Regulation (GDPR) provides the framework for these responsibilities and duties and is commonly referred to as 'data protection legislation'.

There may be other recognised UK or international standards that organisations choose to adopt and comply with in their internal policies, eg the SPECTRUM collection management standard for museums.

Whatever the size of your organisation, everyone must respect others' personal information and keep it secure. Each organisation should set out their approach in their Privacy Notice, which is a key requirement of the data protection legislation. It is the publicly facing statement that explains how the organisation protects personal data and takes its responsibilities seriously. Personal data is any information that by itself or when combined with other information can identify a living person. As well as the obvious email address or name, this can be a CCTV image, car number plate or reference number that links to an account or mailing list.

Some information is regarded as particularly sensitive and has additional security requirements for its handling if it is collected:

- ethnicity
- religion
- medical history
- sexuality
- political views

The risk of non-compliance if such data is lost, stolen or misused, either by accident or deliberately, means reputational risk for your organisation and the potential for sanctions or fines.

This guide from The Association of Independent Museums (AIM) summarises how museums can manage privacy and data regulations. It will be relevant to most heritage organisations.

Understanding what is meant by 'data' can be complex. Through flowcharts and simple stages the Information Commissioner's Office (ICO) has provided a detailed guide.

Managing online security and privacy

Keeping staff, volunteers, and communities – including children, young people and the vulnerable – safe in both physical and online spaces is important to all heritage organisations. In digital spaces, safety can be maintained through effective management of online security and privacy.

As employees and volunteers responsible for collecting personal data, you need to know how to record what you collect, where it is held and how to keep it safe both online and offline. Holding onto informal paper lists of rotas or contact numbers for volunteers needs to be treated with the same care as a formal spreadsheet because each risks breaching personal privacy if left unattended or mislaid. This guide provides pointers so you can be confident that you hold the information only for as long as it is needed and then delete it at the right time. Each organisation needs to have clear processes in place to help employees and volunteers know what to do.

Managing online privacy and security well is also important because trust matters. The reputation of heritage organisations depends upon those we work with having confidence that we take our legal and professional responsibilities seriously.

> **Protecting privacy online is crucial. Not only does it ensure individuals who engage with organisations have their rights respected and their information secured from unauthorised access and exploitation, it also protects the organisations themselves. No one will want to engage with an institution that is careless with their information.**
>
> Jon Card, Executive Director,
> Collections and Governance and Data Protection Officer,
> Imperial War Museums

Useful resources:

Helpful guidance on the basic principles of data protection compliance from the ICO.

The National Cyber Security Centre (NCSC) advice on online safety and security.

Home and remote working

The shift to homeworking due to coronavirus (COVID-19) has accelerated the use of online tools and services by all of us. As well as devices and software that might be provided by your heritage organisation, many of us are using our own personal devices including computers, tablets and mobile phones. We might also use free and low cost web-based services for work we carry out for heritage organisations or projects, including:

- video conferencing
- email
- online storage
- collaboration tools
- social media platforms

Keeping equipment safe

Keep a record of what devices are being used by all staff and volunteers working for your organisation, including the make of the device, model numbers and unique organisational codes. For assets belonging to the organisation, this information will help you trace your devices in case they are lost or stolen and identify any devices that require updates and extra software to protect against any potential cyber security issues.

Where personal devices are being used either in the workplace or for home working, ensure that the same security standards are being followed so that the organisation's data is not at risk. Any details captured about the use of personal devices should only be used for this purpose, and deleted when the business need no longer exists.

Ten steps for better network security from the NCSC.

The ICO has useful guidance on your legal requirements and next steps when working from a personal device.

> **Using digital platforms to engage our audiences during lockdown has been critical to us. We use it as a way of sharing the collection, highlighting how the collection can shed light on the many issues society is grappling with today and carrying out contemporary collecting. Our increased reliance on digital as a means of keeping in touch with local and worldwide communities has also led us to a better understanding of issues around online security and privacy.**
>
> Kylea Little,
> Keeper of History,
> Tyne & Wear Archives & Museums

Software and apps

Software and apps should be updated regularly on all devices used for work purposes, whether they belong to the organisation or are personally owned by you. This will help ensure any sensitive data remains secure. Software companies will update programmes when security issues are discovered, to keep them secure. While some software will update automatically, you might get notifications on your device to manually update – for example, a notice that tells you an update is available for a specific app. Some software may not provide prompts. It's good practice to know what you have installed on your device and routinely check for updates.

> The NCSC has tips on keeping software up to date and securing your devices.

Firewalls

A firewall is a security system that prevents unauthorised access to a private network connected to the internet. A hardware firewall can help to protect groups of computers in a network, and software firewalls can protect individual devices. If you are using a device for managing or accessing information for work, you should install a firewall.

> Further information about firewalls from Get Safe Online.

Acceptable Use Policy

Heritage organisations that provide IT equipment and systems should have an Acceptable Use Policy –a statement about how you use the equipment and clear rules about how your organisation's network, website or system can or can't be used, including Wi-Fi.

> See the ICO's helpful overview for organisations about IT security, including a handy checklist of requirements.

Keeping data secure

You should only collect data that you need for your work, and you should ensure that you know what is being collected and how it will be used, as set out in your organisation's Privacy Notice.

If personal data is collected for work purposes, in order to comply with the data protection legislation, you need to know:

- what personal data you are collecting and why
- where you are storing it
- how you are protecting the data and for how long

Data protection legislation requires you to retain personal data only for as long as it is needed. This will depend on a number of factors, including the purpose of the data and any legal requirements there are relating to the length of time specific types of data must be kept. For example, financial regulations require pension-related data to be kept for as long as an employee is alive, regardless of whether they are still working for your organisation. Some personal data collected might have a very limited use, such as information relating to participants who are attending a specific event. In this case, without additional permissions to contact participants in future, you would need to delete this data after the event once the business need had completed.

> The ICO provides guidance on how long personal data should be kept.

Data breaches

A data breach occurs when personal data is lost, compromised or stolen, whether deliberately or by accident. Under data protection legislation, there is a duty to inform the ICO of a breach **within 72 hours of becoming aware of the breach** if personal data held by your organisation is affected and the subject concerned is potentially affected.

> See the ICO's information about personal data breaches, including checklists for preparing for and responding to a breach.

Back up your data

You can guard against unintended or accidental loss of data by keeping an additional copy, or back-up, of data. There are a number of ways that you can do this. Some services will provide automatic back-ups for you. You should always make sure that you have an appropriate back-up in place. Some data you collect might be irreplaceable – for example oral history interviews. Other kinds of data might be prohibitively expensive or time-consuming to replace.

> A guide to backing up your data from the NCSC.

Work safely with data

- Ensure that people who don't have permission to view confidential, commercial, personal or other sensitive data aren't able to look at this when you are viewing it on your screen.
- Always close your screen if you are away from your computer.
- Make use of security features like password or PIN code protection.
- Set an automatic session time-out on your device.
- Manually log out of sessions if leaving your device unattended or when you leave a shared computer.

Phishing

Phishing attacks are designed to trick individuals into providing access to data or providing information directly. Typically, these will be in the form of emails which ask you to click on links or open files (which allow scammers to install malware on your device), or ask you to provide information like passwords or banking details. Attacks may have a big impact on organisations and constitute serious security breaches, so you should always be careful.

> See the NCSC's guidance on dealing with phishing.

- Never click on unfamiliar or suspicious links in emails, and check to see if emails are really from who they say they are. You can do this by right-clicking or hovering over an email address. See the NCSC's guidance on dealing with suspicious emails.
- If you think you have been the subject of a phishing attack which might have compromised the personal data that you hold for your organisation, follow the steps outlined by the ICO as soon as possible.

Passwords

Reduce the risk of unauthorised access (being 'hacked') and keep your data safe by avoiding predictable passwords and always changing default passwords.

If you have trouble remembering multiple passwords, don't write them down! Use a password manager instead. These applications can generate unique, complex, easily changed passwords for all online accounts and the secure encrypted storage of those passwords.

> The NCSC provides advice on using strong passwords and password managers.

Mailing lists and newsletter sign-ups

Online mailing lists and digital newsletters are an efficient way for heritage organisations to stay connected with their communities. People must give consent for you to collect their personal data, including names and email addresses, and agree to you holding their data for that purpose. You cannot use their data for any other purpose or share that data with others even within your own organisation. People should also be able to easily withdraw their consent, or unsubscribe, at any point. This data must only be held for as long as it is required.

> The ICO provides guidance on using marketing lists and the use of cookies.

Useful resources:

Learn My Way, by the Good Things Foundation includes entry-level courses on keeping your device safe and keeping safe online.

ICO helpline for further assistance regarding privacy

ICO practical guide to online security

This NCSC test will help you understand whether your small- or medium-sized organisation has the basic security it needs in place.

This guide for keeping children and young people safe online by Childnet International for The National Lottery Heritage Fund covers a range of issues that affect everyone.

CILIP and the Carnegie Trust's guide for public libraries in managing data privacy has useful pointers also applicable to heritage organisations.

Home and remote working checklist:

- [ ] Do you know how to keep your software and systems updated?
- [ ] Do you know how to keep your devices and the personal data you are accessing secure?
- [ ] Are you using secure passwords?
- [ ] Do you check before opening emails from unfamiliar contacts?
- [ ] Do you know what personal data you are storing, why, where and for how long?
- [ ] Can you identify and do you know how to respond to a data breach?
- [ ] Are you keeping updated about your online security and privacy responsibilities and communicating this to people you work with and support?
- [ ] Have you sought consent from your users to mailing lists and newsletters?
- [ ] Can users unsubscribe from your mailing lists and newsletters easily?

Using public Wi-Fi safely

Wi-Fi refers to a group of technologies that allow multiple users to access the internet and networks wirelessly. You may use a private Wi-Fi connection at home, or a private connection at work that can only be accessed by members of your organisation. Public Wi-Fi refers to a network connection that is available for anyone to connect to, either with or without a password, typically available in public places like restaurants, shops and airports.

Take care when sharing your home Wi-Fi password

Your network connection could be misused by those gaining unauthorised access to your systems and data, or those who may use your Wi-Fi for illegal activities such as downloading inappropriate or illegal content.

People using guest Wi-Fi should have to agree to an Acceptable Use Policy (AUP)

An AUP sets out what users can and can't do while using your network so that their activity doesn't compromise your organisation's online security. This can be a simple click to understand the requirements but it puts them on notice about acceptable use. Some larger organisations will have filters that provide alerts about inappropriate use.

Always treat public Wi-Fi as being less secure than private networks

Services that don't require registration or passwords should be avoided and regarded as insecure.

Tips for using public Wi-Fi safely:

- Use a computer with a firewall and up to date anti-virus software to protect your computer and its data. This guidance from NCSC explains what anti-virus software is.
- Avoid sending confidential emails, for example those including personal or sensitive data, until you can connect to a more secure system.
- Limit file sharing.
- Encrypt files that contain confidential, personal or sensitive data.
- Limit inputting financial or personal information via any websites unless you are sure that the websites that you visit are secure. This will be indicated by a padlock sign in the web address of all the pages of websites that you visit.

Online video conferencing

Using video conferencing platforms has become part of the daily routine for many people having to work from home. Popular services include Zoom, Face Time, Microsoft Teams, and GoToMeeting. These platforms can be used to host formal or informal meetings, webinars, interviews, teaching sessions or events.

Many heritage organisations are now routinely making use of video conferencing. In December 2019, Zoom had 10 million users and Microsoft Teams had 32 million users worldwide. By the beginning of May 2020, due to the lockdown made necessary by the pandemic and the shift to homeworking, Zoom estimated that it had 300 million participant users daily and Microsoft Teams had 75 million active users globally. For many of us, video conferencing has become something we use regularly to stay in touch with friends and family and to work. Video conferencing platforms enable us to collaborate in real time and share files.

Potential risks of video conferencing

Without using sensible security built into the platforms, video conference meetings have the potential to be hijacked by individuals or groups of people. This is sometimes called 'Zoom bombing', after one of the most popular platforms. People planning to disrupt sessions may have signed up to attend the event and appear to be legitimate participants. Attacks may include sharing inappropriate or illegal content, or showing images or video in the participant window. Collaborative tools may be misused - for example, using a whiteboard or annotating slides to draw offensive text or pictures. Flooding chat spaces by copying and pasting offensive or illegal text is also a common tactic. Audio can be used to broadcast loud noises or obscene comments. This is rare and should not deter from the benefits that video conferencing has to offer.

> **Video conferencing has been an essential tool in the archivist's kit during lockdown – allowing us to continue to train, hone our skills, and keep in touch with our organisations and volunteers, as well as answer queries. However, as information professionals, this incredible usefulness must be balanced against a high regard for GDPR compliance and data security.**
>
> Faye McCleod,
> Archivist and Records Manager

> **With over 100 heritage sites and five offices some staff were spending hours on the road each week. Video conferencing means we can meet colleagues from all over Scotland without the need to travel. This has made the organisation more productive as well as reducing our carbon footprint.**
>
> Susanna Hillhouse,
> Head of Collections Services,
> National Trust for Scotland

Choosing a video conferencing platform

If your organisation doesn't provide a specific video conferencing platform, you will need to decide which service works best for you. Read the platform's terms and conditions before you decide and look at user or community reviews.

Make sure that you understand how the content and/or data you post on the platform will be used, stored and shared. You can find this information in the service terms and conditions – all services should have a privacy policy.

Find out how recordings and data, including chat facility content, will be kept secure and what procedures the platform has in place to tell you about any data breaches.

You can also find comparisons of video hosting platforms security and privacy features online. These tend to date very quickly as services are updated constantly, so be sure to check the date of the comparisons. Check that the comparison comes from an objective third party.

Your organisation might have policies that restrict or determine the platform you use, or privacy rules that can help you decide.

Collecting participant data

If you are hosting a meeting or activity that is open to the public, ask people to sign up in advance and register. This will enable you to provide any information about the meeting, and get agreement for expected behaviour and consent for any recording taking place. You can choose to provide individual log-in links to the webinar or meeting for additional security.

Remember, as with all personal data you must only keep names, email addresses and job titles for the purposes of the meeting, and it must be deleted after the meeting. You must obtain permission from attendees to hold their data for any other purpose, eg alerts to similar events.

Before your meeting starts

Friendly space policies

Many organisations have friendly space policies or codes of conduct that they ask people to agree to before attending in-person and online events. These make sure people are clear about the kinds of behaviours that are expected from participants, and what the consequences of not adhering to community standards are. It's good to ask participants to read these before meetings, and state that attendance is taken as a sign that the participant agrees to these.

Codes of conduct are a way that organisations can demonstrate that they value the participation of all members of their community, ensuring everyone feels welcome. If possible you should develop your code in consultation with your community.

The Wikimedia Foundation have shared their implementation steps and some sample agreements.

Some dos and don'ts of online behaviour from Childnet.

An example of a code of conduct for online events (NSCS).

Recording meetings

Are you planning on recording the meeting, or saving the text chat from the meeting, or both?

For example, will the text chat be captured by the video, or will you save it as a text file? If so, you will need to seek consent from participants in advance and remind them during the meeting. They will also see the recording sign on the screen, which will act as an alert.

Will you be live streaming the meeting via another platform such as YouTube?

Check the terms and conditions of the platform you are using and make sure that you have the consent of your participants if you are including them and/or chat facility comments. Check that use of any additional platforms doesn't compromise the security of your main platform, or present additional security issues you need to be aware of.

Will you be posting the recording in public after the event?

Will you be publishing text chat conversations that took place during the meeting? You will need to seek permission from participants in advance.

How long are you planning on keeping a copy of the recording for the internal use of your organisation?

If you post a video publicly, will you take it down at some point? Make sure your participants are aware of this so they can provide consent, and this is set out in your internal policy about storing data.

Meeting room management tools

- Consider how you might want to manage your participants' interactions in the online meeting. Most video conferencing platforms will let you choose whether you allow participants to use a chat facility and whether they can share their screens. The host of the meeting will be able to mute participants' microphones and control whether participants are able to use their cameras.

- Make sure, as host, that you know how to turn off video, mute participants, delete chatroom content, and eject participants.

- Set up a password or a waiting room facility for meetings involving people from outside your organisation. Set up each meeting with a new password and share it only with participants you know are joining you.

- Using a waiting room option means that you can manually let people into the session. This gives you greater control over who is in the room, but takes more time, so isn't always a practical option for big meetings.

- When recording any of the participants (including external speakers) and/or any of their live chat, ensure you have the appropriate consent to record them and then to broadcast or publish the broadcast. It is particularly important that you seek consent from parents or guardians of children and vulnerable adults. See the ICO guide to seeking and managing consent.

Starting your meeting

- If you have the chat facility enabled, explain to participants how to use it, who can and can't see messages they send to each other, and whether private messages can be viewed by moderators.
- Remind your participants if you are planning on recording the meeting, if you will be recording or saving any of the public chat, and what you will be doing with any recordings or copies.
- Under data protection legislation, additional requirements apply to vulnerable participants using online services or educational resources. If any members of your group are under 13 years old then additional safeguards are required to manage their personal data, including age-appropriate instructions and design and parental consent. The ICO provide information on managing children's data.
- Remind your participants about the behaviour you expect from them and highlight key requirements outlined in your code of conduct, eg not allowing others to take screenshots without permission.

During the meeting

- Having other people to help moderate and manage an online event can help things run more smoothly, and ensures that if anything goes wrong there are people on hand to spot it and deal with it quickly. If you enable chat during the meeting, make sure you have at least one other person with you to keep an eye on it.
- Any behaviour that is in breach of your code of conduct should be dealt with promptly. Where necessary, participants who breach behaviour rules should be removed from the meeting.
- If you are recording the meeting, switch off the recording functionality before and during any breaks. Remind participants after any breaks that the recording has resumed.

After the meeting

- Delete any registration data about the participants, unless you have permission from them to retain it and a clear reason to continue to hold it.
- Delete the recordings themselves when you no longer need them. If the recordings contain any content that breaches privacy (for example, images of children for which permission from parents or guardians has not been sought) or infringes copyright, or any content which is illegal, you will have to remove that section of the recording. If this is not possible, you will not be able to post the recording.

Useful resources:

NCSC guidance on video conferencing

ICO guidance on video conferencing

Online video conferencing checklist:

- [ ] Have you read through the security and privacy statement provided by the service you are using?
- [ ] Do you have a code of conduct in place, and know how you will share this with participants?
- [ ] Is the host in control of the features and controls?
- [ ] If you are going to record the session, have you got consent from meeting participants, including any speakers?
- [ ] Do you know how all the security and privacy features work, and how to set these up prior to the meeting? For example, password protecting your session or using a waiting room.
- [ ] Do you have a plan in place in case your event is disrupted by offensive or illegal content or conduct?
- [ ] Have you treated any data you may have collected in line with your data protection responsibilities?

Social media

Social media platforms like Facebook, Twitter and Instagram enable individuals and organisations to communicate in real time to connect and engage with communities. They can be used to host educational events and talks and for marketing and promotional activities. They can be particularly useful when access to physical heritage spaces may be restricted.

It's important to know how much personal data we post, how we stay safe online and guard against cyber crime, and how we can protect the communities we support, particularly those that include children and vulnerable adults. In this way, we can get the most from social media, but reduce the risks on criminal activity and comply with our data protection and other legal responsibilities.

The National Lottery Heritage Fund/Childnet guide to working with children and young people online includes tips on working safely in social media environments.

Even if your audience is primarily adults, you should be mindful that there might be young people across all public online spaces.

- Make sure you understand the privacy settings of any platforms you use, as well as how to report inappropriate or illegal content. The NCSC provides information about privacy settings across the most common platforms.
- Familiarise yourself with common privacy issues, for example, sharing personal details or photographs of others without their permission. The ICO has helpful guidance with examples on the use of social media and online platforms.
- Children aged 13 and over can create their own account on most mainstream social media platforms. See Childnet's guidance about young people using social media platforms.
- Many organisations have a social media policy which provides guidelines on what employees should be aware of, and what they should avoid doing, on social media.

The National Council for Voluntary Organisations has provided guidance on creating a social media policy.

The ICO's own social media policy provides a good template for organisations.

Charity Comms, the membership network for UK charity communications professionals, also has a social media policy template.

> **Visual images of participation in our work are key to social media. We always seek permission to use images of our participants at the outset of a project so we are confident we don't infringe their privacy and break data protection rules.**
>
> Emma Larkinson,
> Operations and Development Manager,
> Craftspace

> **Using social media has been a lifeline over the last few months. It has enabled me to connect directly and personally with established users and new audiences. Social media may be a rapid form of communication but you must always think, reread and consider the audience before posting!**
>
> Heather Dawson,
> Academic Support Librarian,
> LSE Library

Further resources:

ICO information on privacy and social networking sites

Advice on parental controls from Internet Matters

Next steps: continuing to manage risk

- Keep up to date about your responsibilities regarding privacy and online security by attending regular training and awareness sessions. Introduction to cyber security: stay safe online is a free online course from OpenLearn, developed by The Open University with support from the UK Government's National Cyber Security Programme.
- Know how you can work from home and stay safe online. The Prince's Responsible Business Network's at-a-glance guide links to free cyber security e-learning, home working guidance and small business resources.
- Sign up to the ICO newsletter and NCSC updates for the latest information about privacy and online security.
- Regularly review your digital security and privacy arrangements, specifically how and where personal and sensitive data is stored in order to effectively assess and manage security risks.
- Know what to do if you suspect a data loss and need to follow security breach procedures. This will enable you to respond quickly by alerting colleagues and where necessary reporting to the ICO within the required 72 hours.