Appendices

Appendix A: Model gift agreement

THE AGREEMENT

This Agreement dated DATE is made between NAME OF ORGANISATION ('ABBREVIATED NAME') of ADDRESS OF ORGANISATION, on the one part; and the Donor identified in the Schedule on the other part.

The following are the terms and conditions upon which the Donor now agrees to place the material identified in the Schedule to this Agreement ('the Papers') with the NAME, and the NAME agrees to accept the placement.

1) Ownership of the Papers

i) The Donor represents and warrants that he/she is the owner of the Papers.

ii) Ownership of the Papers which will be placed exclusively with the NAME will be vested in the NAME; and title to any Papers placed after the date of this Agreement will transfer to the NAME on delivery.

2) Access

The parties intend that after cataloguing the Papers will be made available to the public for research purposes but they recognise that in some cases items may be confidential; others may contain personal data; and others may be so sensitive that their disclosure could endanger individuals' health or safety.

Such items will be identified either before placement with the NAME and indicated in the Schedule, and/or marked in the process of cataloguing, together with a note of the period of reservation. If the NAME receives a request under the *Freedom of Information Act 2000* for the disclosure of information in the Papers/Manuscript(s), the NAME will notify the Donor and consult with the Donor.

Subject to the Act, it is the parties' intention that until catalogued the Papers should remain closed to all but members of staff at the NAME and authorised representatives of the Donor. After completion of the catalogue, members of staff at the NAME will consult with the Donor about on-going arrangements for access which comply with the Act.

3) Intellectual Property Rights

i) All and any copyright in the Papers is held exclusively by the copyright owner(s), unless otherwise assigned.

ii) The Donor will not dispose of the copyright in his/her lifetime.

iii) The Donor permits the NAME to store, translate, copy and re-arrange the Papers electronically for the purposes of preserving the digital items in the Papers.

iv) The Donor permits the NAME to create catalogues of the Papers and to create metadata required for the preservation of digital items in the Papers. The NAME will own the copyright in the metadata, any copyright in the catalogues which can be distinguished from copyright in the Papers and any database rights in the catalogues. The Donor shall be provided with a copy of any such catalogues.

v) The NAME will not reproduce or sanction to be reproduced by mechanical means (including all forms of photography) any material without the express permission of the copyright owner(s). As an exception, however, the Library staff may use their discretion to supply copies to applicants who have signed a standard copyright declaration

agreeing (amongst other conditions) to use the copies solely for purposes of non-commercial research and to seek the permission of the copyright owner(s) for any other use.

vi) In the case of such mechanical reproduction, the NAME will hold copyright in its own images (e.g. transparencies or digital files), but without prejudice to the underlying copyright in the material and any permissions granted to the NAME for the use of the material.

4) Disposal

i) The NAME reserves the right to return to the Donor any material not deemed of archival value or, with the consent of the Donor, to destroy such material.

ii) In the event that the NAME wishes to de-accession the Papers, the NAME agrees not to sell, move or otherwise dispose of the Papers without consultation with the Donor, his/her heirs or assigns.

5) Preservation

The NAME will exercise the same degree of care over the preservation of the Papers as over the preservation of similar property of the NAME which is kept in the NAME.

6) Loss or damage

The Donor appreciates that, except as stated above, neither the NAME nor any of its officers, employees or agents can accept responsibility for loss or damage to the Papers.

7) Security

The NAME agrees to take reasonable measures to prevent unauthorised access to, duplication of, or distribution of the Papers.

SCHEDULE

The Donor

Name: NAME OF DONOR, his/her personal representatives and those entitled under his/her estate to the copyright in the Papers referred to below

Address: ADDRESS OF DONOR

The Papers/Manuscript(s)

(a) DESCRIPTION OF PAPERS:- e.g. correspondence, manuscript(s), notes, speeches, writings, photographs, printed material, digital material, videos cassettes:

(b) Reserved Papers/Manuscripts (if any):-

description:-

period of reservation:-

reason(s) for reservation:-

(c) Further material which may be donated by the Donor in future:

AS WITNESS the hands of the Donor and of an authorised signatory for the NAME:

SIGNED for and on behalf of NAME Name: _____ Position:_____ Signature: _____ Date: _____	**SIGNED BY** NAME AND ADDRESS OF DONOR Signature: _____ Date: _____

Appendix B: Guidelines for creators of personal archives

Caring for your personal digital archive

Archivists often become involved with a personal archive after the retirement, or even death, of its creator. A paper-based personal archive can be left untouched for generations with little impact on its future viability; as long as the material is simply arranged and suitably stored it can be used effectively over many decades. The same cannot be said for the increasing amount of material that now exists solely in digital form. The long-term viability of unmanaged digital material is uncertain, and efforts to keep material accessible in the medium-term can be frustrated by hardware, software and media degradation and obsolescence.

Time is of the essence. The fragility of digital materials in our fast moving world is well documented. To ensure continued access to your digital materials in your own lifetime and to pass these digital materials on to future generations, you need to act now.

To maximise the chances of your digital material surviving for as long as you need it, it is important to learn new ways of managing that material. This document aims to assist you in doing just that, by providing practical advice that can be implemented by anyone.

Why should I bother managing my digital materials?

Because their survival is far from assured...

Not so long ago, personal records documenting the early years of an individual's life might be preserved in suitcases on the tops of wardrobes or in shoe boxes in the attic. The personal archives of eminent people often include christening photographs and school work. The digital equivalents of such valuable records for individuals born at the start of the twenty-first century will not survive this benign neglect. Even if copied to a CD and placed in a shoebox their survival is unlikely - while CDs may take decades to degrade, the hardware required to read them and the software required to render the file formats may have long since become obsolete. Many of us are all too familiar with the loss of such irreplaceable digital artefacts – sometimes only a comparatively short time after their creation. The time is near when the family photograph album, now lovingly handed down from generation to generation, is likely to exist only in digital format. Without active intervention it is unlikely to become an heirloom, or even survive the next software crash. The same is true of audio and video recordings, correspondence and personal websites.

Because your digital materials are important to you and your family...

Managing your digital materials will ensure that weeks spent slaving away at a piece of work isn't wasted because of a hardware failure perilously close to a deadline; it will safeguard the personal memories captured in photographs and email correspondence that will intrigue future generations of your family. Some digital materials fulfill practical, often professional or administrative, needs; others provide mementos of people, places and times which are more personal. All are important parts of your personal archive; ensure that they are available to you when you need them, whether 'when' means now, in a few months, in a few years, or even in a few decades.

Because your digital materials are important to society...

You may not have thought of your digital files as part of a personal archive, or as having long term historical interest, yet what seems ordinary and mundane to you now may well interest future researchers. In an archival repository, your archive will reveal a personal perspective on your life, work and environment for posterity; it will combine with the mementos of your contemporaries, forbears and successors to provide personal and historical insights into past times.

Where can I get advice about my archive?

These guidelines are one source of advice; family, friends, an employer, or even the media are others. If you intend that your archive should make its way to an archive repository for permanent preservation, then it is a good idea to get in touch with your chosen repository sooner rather than later. You could arrange to make regular transfers of your digital archive to the repository, or simply take advantage of the repository's curatorial expertise to manage your own archive in situ. While these guidelines provide some useful generic advice, digital archivists can offer more specific and up-to-date guidance that is tailored to your record keeping habits and preferred technologies.

Various collecting institutions, ranging from local authority archives and museums to university archives and specialist repositories, might be interested in your archive. While some of these are interested in recording a representative sample of all individuals, most have specific collecting priorities such as the papers of politicians, modern literary authors or scientists. You can locate repositories which might be a suitable home for your archive by looking at the collecting policies of likely institutions (these are sometimes published on an institution's website), or by contacting the National Advisory Services[1] at The National Archives who can offer advice on suitable places of deposit.

Practical tips

The maintenance of your personal digital archive is an ongoing task. Fortunately, by adopting good practice at the outset, it does not take too much effort to increase the longevity of your digital material! Individuals have a variety of record keeping behaviours, ranging from those who purge to those who hoard, and from those who organise to those who live in a state of semi-chaos. Most of us fall somewhere between these extremes and you will know best what fits your style. Below is a series of practical tips to help you maintain your personal digital archive. It is important to choose solutions which suit you, so adopt - and adapt - these according to your needs. The tips range from making conscious decisions about naming and format when you create a file, to the deletion of low value material in order to free up storage space and make it easier to find what you are looking for. There is also advice about backing up, and administering and caring for your computers; and for safeguarding both your own privacy and that of others. Simple measures like these can have a dramatic impact on the survival and utility of your digital archive. These tips are not intended to be prescriptive. Although some of them may seem time-consuming, in reality most involve small changes to the way that you work that should reap benefits in the years to come by ensuring both that your important digital materials are still accessible for as long as they are useful to you and that you can find them when you need them!

1. Organise and name files appropriately

Most of us accumulate material in a haphazard fashion and do our best to impose some basic order that will help us rediscover items for future needs. Remember that search and discovery tools can only do so much; they cannot tell you why you created a document, or explain unfamiliar abbreviations and acronyms. Making your documents transparent will help you to understand them in the longer-term. Here are a few tips you could try to make it easier to find important materials quickly.

Naming files and folders:

- Be concise: avoid long and complex file paths.
- Select meaningful names: this facilitates searching and browsing.
- Develop standard naming conventions for the file names of record types you create or save on a regular basis.
- Avoid capitals or spaces: this can cause problems when moving files between different computing environments.

1 The National Archives, 'Advice to Private Owners', *The National Archives website.* URL: <http://www.nationalarchives.gov.uk/archives/advice_private_owners.htm>

- Use the format yyyymmdd (e.g. 10 June 2005 = 20050610) for recording dates: that way your files will be presented chronologically in file management tools.
- Adopt a version control system for drafts (e.g. yyyymmdddocumentname-2.pdf, where -2 denotes that this is 'version 2' of the document). This prevents the embarrassment of sending the wrong version of a document to others. Drafts are also valuable for researchers tracing the creative thought process.

Make your data self-documenting

- File related information together in well-named folders, which give an indication of the subject, project or activity on which they are based.
- Add information to the body of digital documents which explains them to a general audience. This can help you when you re-discover a document too. Simple information, such as a log of authors, a document history and a note about the purpose of a document can be very helpful. You could add a simple table like this to any textual document:

Document Title	Caring for your personal archive		
Author(s)	A.N. Other and A. Colleague		
Purpose	Provide guidance to individuals wishing to preserve their digital materials for their own use and for placement at an archival repository.		
Date	01/02/2007-	**Filename**	20070201sample-doc-2.odt
Access	Internal	General dissemination ☑	
Document History			
Version	**Date**	**Comments**	
1	01/02/2007	Document created by A. N. Other	
2	31/03/2007	Revisions to language by A. Colleague	

- Most desktop applications include a 'properties' option containing file metadata (e.g. title, location, size, dates last accessed and modified). Some of this is generated automatically, but you can record extra metadata yourself, e.g. keywords or a free-text description.
- For images: if your camera or related software allows you to add metadata to your images (i.e. information about when and where a photograph was taken, and what or who it depicts) at point of capture or export, then use this function. This will help you to find photos of particular times, people, places and events. Save photos in purposely created folders rather than randomly in the default 'Pictures' folder and consider saving a simple text file describing the background context of the images (date, place, people, etc.) alongside them.
- When saving documents from the Web for reference purposes, make a note of their source: web addresses can change, and if you want to cite a document in future it is useful to have a record of where you obtained it from and when you last accessed it at that address.
- File email attachments you wish to keep separately rather than leaving them in your email directory. It is useful to identify their source as email attachments in their file name, or even to save a copy of the email alongside the attachment.

Delete what's not important.

- Some materials you'll want to keep forever as part of your archive. Some you might need for a few years. These are the materials that should be maintained. Don't waste time and space on material that has outlived its utility: it will make backing up a chore and make it difficult for you and future users of your archive to extract meaningful information from the resulting mass of data.

2. Manage your emails

Email is an integral part of our personal and professional lives and many of us maintain multiple email accounts. An email client is essentially a program that accesses email stored on a server and is used to send and receive email messages. Choosing which email client to opt for is a matter of personal preference; well known examples include Eudora, Mozilla Thunderbird and Outlook Express. There are two main protocols used by email clients accessing mail over the Internet: POP3 (Post Office Protocol) or IMAP (Internet Message Access Protocol).

A POP3 client usually downloads email from the server to your PC and then deletes the email from the server. This means that email messages are more vulnerable to loss, so all the advice on creating backup copies given in Tip: 4 should be followed.

An IMAP client accesses emails on the email server and normally leaves them there rather than deleting them; this means that you usually stay online whilst reading, composing and sending mail. IMAP also allows you to work offline: you can download copies of the messages while the real messages are left on the server. Most modern email clients and servers support both of these standard protocols.

There is a single standard (RFC 2822) for the transmission of email messages; some proprietary email clients convert the standard file into a proprietary database format for storage, which can make it difficult to access the messages if the client becomes unavailable. Email clients that save in the open standard format MBOX include Mozilla Thunderbird, Mulberry and Sylpheed. For a comparison of email clients, see Wikipedia.[1]

In recent years there has been a move towards web-based email services; commercial examples include Gmail and Yahoo! Mail. Webmail can be accessed using only a web browser; no specific email client is required. On the whole, the functionality and flexibility of email clients leave current webmail services a way behind. Not all webmail services provide POP3/IMAP access for downloading email (and some that do charge), meaning that you require a permanent Internet connection to read your email. Choose a service which provides free POP3/IMAP so that you can read email offline and extract it from the service when you need to.

Regardless of the type of email you use, you should manage your email efficiently; often email clients provide inbuilt facilities to help with mailbox organisation. The following list provides some tips on managing your email which should enable you to find the information you need more easily and facilitate future appraisal by a digital archivist:

- Delete email that has no long-term value as soon as possible.
- Don't ignore your sent mail folder: delete irrelevant mail and move sent messages to relevant folders on a regular basis.
- Retain in your inbox only those messages which you haven't yet responded to, or which relate to ongoing business. File or delete the rest as soon as possible.
- Organise your email into subject folders with concise and relevant titles.
- Give email messages meaningful and concise subject-lines that are relevant to the message content. If the subject of an email exchange changes, change the subject-line.
- Respond to emails in a solid block of text rather than inserting text at various points in the original message. The message might be clear to you, but subsequent changes in the technical format of the email (e.g. as a result of preservation activities) can obliterate the clear distinction between original message and annotations.
- Separate personal and professional email if you can. If you use a work-based email account for personal email correspondence, keep non work-related mail in a 'Personal' folder. Protect your privacy by making it clear what is private.

1 Wikipedia, 'Comparison of e-mail client', *Wikipedia website*. URL: <http://en.wikipedia.org/wiki/Comparison_of_e-mail_clients>

- If you receive an encrypted email, decrypt it before saving it; this will facilitate access to it in the future when the email directory is archived. Encrypted e-mails might become inaccessible over time as the method of encryption becomes obsolete.
- Include enough information in your email directory to identify the individuals represented. Your email address book or contacts list is a useful tool for recording information about frequent correspondents.
- Use a spam filter and do not open any email or attachment if you suspect it is spam; attachments in particular are often a source of computer viruses.
- Save covering e-mails relating to attachments you wish to keep; this will provide contextual information about the relationship between message and attachment.

3. Select suitable formats and software

A key factor in increasing digital longevity is selecting the simplest format available for the purpose. The more complexity in a file, the more dependencies it has and the risk of file corruption increases. It is also important to choose formats which are supported by multiple applications. Avoid using confidential proprietary formats where you can; instead, try and use open standard formats. If the file format specification is openly published, the probability of your documents surviving to be read in future years increases significantly. The ubiquity of some software packages (like Microsoft's Office 2003 suite) makes them all too easy to use, but their specifications are opaque, making it impossible to gain a thorough understanding of how they work. Whilst some developers of proprietary formats publish their specifications (such as Adobe PDF), confidential proprietary formats which can only be read in conjunction with specific software are less dependable than publicly available formats which can be read by multiple applications.

Where your work is of a type that currently has no associated standard format, consider using open source software (OSS), where the program (source) code is available. This provides an effective format specification. OSS is also often linked to licence agreements which make it easy to take preservation measures (such as saving copies of the software or migrating to new formats) without violating the intellectual property claims of the manufacturers.

Other advantages associated with OSS include:

- Lower acquisition costs.
- Reduced hardware costs: OS operating systems can run effectively on lower specification machines than proprietary equivalents.
- Reduced risk of hardware obsolescence: the transparency of OS operating systems like GNU/Linux means that they can be used in limitless alternative hardware environments.
- Long-term comprehension and re-use of data is made easier.
- Help for data creators is widely available within the open source community.
- Less risk of malicious attacks than proprietary software.
- Opportunity to provide feedback to improve the software.
- Open source technologies often compare favourably with their proprietary peers in terms of performance and reliability.

More information is available from OSS Watch,[1] a body which offers guidance on OSS to UK higher and further education institutions.

Some suggested formats that will facilitate long term preservation and access can be found below.

1 OSS Watch, *OSS Watch website.* URL: <http://www.oss-watch.ac.uk/>

a) Textual documents

Office suite:

For word-processing try using the OASIS Open Document Format (ODF) which is a published ISO standard (ISO/IEC26300) and therefore more 'preservable' once archived. You can use many applications, including OpenOffice.org,[1] to create and save documents in ODF and a plug-in for Microsoft Word which allows the program to open and save documents in ODF format is available.

Databases:

MySQL, PostgreSQL and Firebird are examples of open source databases, which run on a range of platforms, including GNU/Linux, Mac OSX and Windows, and compare favourably to their proprietary equivalents, particularly in terms of speed and stability. Many desktop applications, including OpenOffice.org can be used to access these database engines.

PDF/A:

PDF is a file format widely used for presentation copies of office documents which cannot be edited by those viewing the file. PDF stands for Portable Document Format (PDF) which aims to provide a mechanism for representing electronic documents in a manner that maintains their visual appearance, independent of the tools and systems originally used for creating, storing and rendering the files.

The 'A' in PDF/A stands for 'Archive' and signifies that the format has been confined to basic PDF features to simplify its long term preservation. PDF/A is not a magic bullet for preserving digital records, although its adoption will assist the preservation of PDF files by preventing encryption, digital rights mechanisms and other features which impede preservation. PDF/A was ISO-approved in 2005 (as ISO 19005-1).

b) Raster images

Raster images are made up of thousands of millions of single dots of colour (pixels) arranged in a grid. They are the kinds of images most often created by digital cameras or scanners.

Some cameras use a proprietary 'raw' format; such formats can be manipulated by software provided by the camera company, but may fall foul of software obsolescence over time. You should therefore save high quality master images (min. 300dpi) in TIFF format, which is a well-supported open standard. If sending pictures via email, or adding them to a website, create lesser quality, but more easily transportable 'throwaway' versions in JPEG format.

c) Email

Think carefully about the service your web-based email account provides; make sure that it is easy to download your email (in bulk and preferably retaining any filing structure you put in place) if you need to. If you intend to place your correspondence in a research institution, you will need to be able to extract it from the email client you download to. Use a client which can save your email in an openly documented format such as MBOX.

d) Websites and weblogs

Comply with W3C recommendations and make sure your (X)HTML, CSS etc. is valid. Select open standard formats for images, audio and video, etc.

e) Operating systems

Your operating system is the central software program within your computer system; it manages all the other programs (known as applications). Apple OS, GNU/Linux and Microsoft Windows are mature, stable and usable platforms.

1 OpenOffice.org. URL: < http://www.openoffice.org/>

4. Backup your files

Hard disks fail. It is not a case of 'if' but 'when'. Your software and files could also be lost as a result of flood, fire or power surge; theft is another risk, especially if you use a laptop. This means that regular backing up of records is an essential task. Consider:

a) Making copies on portable media

An external solid state drive is a good option; these are easy to use, inexpensive and provide sufficient capacity for many people. You could use CD-Rs or DVD-Rs, but this will be more time consuming and may result in splitting data over several disks. You should update your removable media as needed; old media can degrade or become inaccessible as technology evolves.

b) Storing a copy off-site

For key files you could make additional copies and store them elsewhere, perhaps with a friend or relative or in a deposit box. If you have a broadband connection, there are many online services which allow you to upload your files, a form of off-site storage. Always read the terms and conditions carefully and check the following:

- Charges: are there any? What happens if you miss a payment?
- Storage limits: is there a limit to the storage you can use? Is this an absolute limit or a limit to what you can upload on a monthly basis?
- File types: does the service accept all kinds of file type?
- Structure and searching: does the service allow you to retain your file structure? If not, what facilities does it have to ensure that you can find your documents and do they work outside of the service?
- Sustainability: has the service got adequate financial backing? If it fails what would happen to your data?
- Scalability: many of these services are currently small; will they be able to keep up with demand?
- Ease of use: How easily and quickly can you upload files?
- Security: does the service offer secure storage and transfer? How secure?
- How long will your data be stored? If a service claims 'forever', ask what is meant by this claim. How exactly do they plan to achieve this? Never forget that keeping a file forever won't guarantee that it will be usable in ten years time let alone a hundred!
- Reclaiming what's yours: how easy is it to get your data back? The services need users to be viable; it's not in their interests for you to extract your data - it may be more straightforward to transfer your bank account than to remove your data.
- Support: is there support available if you need it? Are there FAQs on the website?

c) Using data synchronisation services or software

If you use several different computers, you probably encounter the problem of not having the right file in the right place from time to time. Data synchronisation services can solve this problem by replicating changes to data on one of your computers to all the others you use. This means that you always have access to your data, and you always have one or more backup copies of your data. The difference between this type of service and online backup services is that your data is not permanently held on third party servers, but is encrypted and sent to your other devices for storage. Again, you will need to check the terms and conditions of services carefully.

The first time you synchronise your data, it is likely to take a great deal of time. After this first sync, only the differences in the data are synchronised, which makes synchronising much quicker.

Read the small print and check the following in relation to services:

- Charging: is it free, or is there a charge? Typically the free services only allow you to process a small number of files a day, so a paid-for service may be a better option.

- Transfer limits: is there a limit to the transfers you can make? Is it limited by quantity of files or file size; is the limit generous enough? Is there a limit to the number of computers you can synchronise to?
- Remote access: will the synchronisation service allow you to access the data on your computer remotely?
- Sustainability: has the service got adequate financial backing? If it fails what would happen to your data?
- Flexibility: does the service or software lock you into an operating system or ISP?
- Scalability: many of these services are currently small; will they be able to keep up with demand?
- Ease of use: does the service allow you to perform batch operations? How quickly can you transfer files to your other computers?
- Security: does the service encrypt your data in transit to keep it secure?
- Network drives: does the service support synchronising of network drives?
- Online: must the computers which are to receive the synchronised data be switched on and online at the time of transfer from the sending computer or can they update when they are switched on and online? Where is the data stored in the intervening period?
- Support: is there support available if you need it? Are there FAQs on the website?

Deciding what to backup
Files which would be difficult or impossible to recreate are the most important to backup. For example:

- Digital photographs.
- Email and email address book.
- Data relating to personal finances.
- Professional or business data.
- Licence keys for software (and software, where allowed).
- Digital music or video that you have purchased.
- Your diary or Personal Digital Assistant (PDA).
- Your website.
- Anything else that is personally important to you or your family.

Make a list of what you intend to backup and decide on a backup routine (how often you will backup which files and to what). If you keep a record of your backup and label the media to which you backup, then restoring your system from your backed up data will be much easier. If you delete material that you don't want, and organise files logically, this will also simplify backup.

For added security, you may wish to consider encrypting your backup data. See Tip 7 for more information on encryption.

Backing up your website
Ideally copies of personal websites should be made prior to major changes and updates. If you are the webmaster of your own site and have access to the files which make up the website, then simply create archived versions of your website by compressing these files into a tar or zip file, using a naming convention such as website20060819.zip; store these in a folder with other archives of your website.

If you create your website or weblog using a service, perhaps the easiest method of archiving it would be to capture a copy of the website using Adobe Acrobat Professional,[1] or HTTrack.[2] Alternatively, you could suggest that the UK Web Archiving Consortium archive your website by completing their submission form at <http://info.webarchive.org.uk/cgi-bin/submission.cgi>, or submit your website to the Internet Archive at <http://www.archive.org/web/web.php> (you must register to do this).

If your website is database driven, preserving it is more complex, as a copy of the database needs to be captured with the website backup. Speak to an archivist, who will be able to advise you.

5. Look after your hardware and media

Accept that your PC and storage media will fail. Organisations replace PCs, servers and storage media on a cyclical basis; you should too. Replace them before they break and avoid losing your data; five years is currently a reasonable life expectancy for hardware and media.

Minimise the failure of computer components and storage media by keeping them clean and preventing them from overheating. Vacuum dust that collects on your computer equipment and keep air vents clear. If your computer's fan is struggling to cope with the heat, then shut down the computer and postpone unnecessary work. Make sure that hardware and media are stored in stable environmental conditions, and not precariously perched on unsuitable desks or shelving. To avoid data corruption, USB keys and other mass storage devices such as MP3 players and digital cameras should be correctly removed from hardware according to the needs of the operating system. CDs and DVDs should be treated with care to prevent damage.

Invest in a small Uninterruptible Power Supply (UPS). A UPS protects from power surges. The better ones also smooth voltage peaks and troughs, and in the event of a power outage will continue to supply power to your PC allowing it to be shut down gracefully, and avoiding data corruption.

6. Administer your system

Before undertaking major updates of hardware and software take some time to think and plan your actions. It is common for older files to get lost as a result of updates. Files should be backed up elsewhere prior to hardware and software changes.

Be security aware. Unless you are certain your operating system doesn't need it, then anti-virus software and a firewall should be installed and regularly updated. It is important that you do not open suspicious emails or attachments. You should also be aware of the various kinds of 'badware' (like spyware, malware and deceptive adware) which can affect your system. If you are plagued by pop-up ads when online, it is likely that you have badware on your computer; badware can ultimately cause your system to crash and can also lead to the abuse of your personal information. You may be unaware that you have downloaded badware, which can be loaded onto your system when you visit certain websites; sometimes it is even included in proprietary software packages, with no acknowledgment of this on the part of the manufacturer.

Useful information is supplied by the Stop Badware Coalition,[3] a 'neighbourhood watch' campaign aimed at fighting badware.

7. Consider using passwords and encryption devices

If you keep valuable and personal data on portable media, PDAs, or laptops it might be appropriate to consider encryption as a means of keeping data safe; imagine if your laptop were stolen, what kind of valuable, private or even embarrassing information it might contain.

There are many different kinds of software that can encrypt files, folders, emails, attachments, portable storage devices and more. It is best to select open-source encryption software to ensure continued availability. One example of open source (free to use) disk encryption software for Windows XP/2000/2003 and GNU/Linux is TrueCrypt.[4]

1 Adobe Acrobat 8 Professional. URL: <http://www.adobe.com/products/acrobatpro/>
2 HTTrack Website Copier. URL: <http://httrack.com>
3 StopBadware.org, *StopBadware website.* URL: <http://stopbadware.org/>
4 TrueCrypt. URL: <http://www.truecrypt.org/>

If you habitually use encryption, it is important that you remember your passwords; a lost password can render your data inaccessible. One solution is offered by password managers. Software like KeePass[1] enables you to manage your passwords in a secure way. You can put all your passwords in one database which is locked with a single master key or key-disk, so you only have to remember one master password or insert the key-disk to unlock the whole database.

It will become increasingly important for those with valuable password protected or encrypted digital assets to make provision for their access in the event of the creator's death. Relevant details should be stored offsite in a secure location, perhaps lodged with a solicitor or kept in a deposit box known only to likely executors.

8. Be aware of intellectual property rights and privacy

Copyright and licences

In addition to the documents you have created yourself, your own digital archive will inevitably include material (reports, articles, images, music, etc.) created by others. This material (whether officially 'published' or not) will usually be subject to copyright legislation, so you should be careful about how you use it; copying, editing or forwarding copyright material could be a breach of copyright law. Where you do hold digital material which was created by other people, it is useful to be aware of who authored particular documents and when they were created. This information will help the future curators of your archive in determining the copyright status of the material. When you donate or deposit your archive with an institution, the digital archivist is also likely to ask you for permission to make multiple copies of the digital material in which you hold the copyright, for preservation purposes.

Copyright applies to your unpublished written works for 70 years after your death. If you want to encourage greater usage of your digital archive, you could consider applying less restrictive licences to your material, using licences such as those developed by Creative Commons.[2]

Digital Rights Management

It may be that documents which have come into your possession are covered by proprietary Digital Rights Management (DRM). Windows DRM, for example, can be applied to word processors, email clients and other applications; it enables you to choose from a variety of usage rights to define who can open, modify, print, forward, or take other actions with the information. These usage rights are locked within the document itself, controlling how information is used even after it has been opened by intended recipients. Similar digital rights management functions can be attached to Adobe Acrobat products – allowing publishers to control the opening, display and use of files. Other packages also come with such rights management facilities.

One problem with DRM systems is that they are not time limited in the way that copyright law is, meaning that even when the copyright in a particular digital work has expired, there is currently no easy mechanism to remove the copy control systems embedded in the work. This is a major problem for archivists of digital material because undertaking proper digital preservation measures requires them to copy or migrate it into different formats. It is also a barrier to future access by researchers; once material is in an archive, even if still in copyright, it can ordinarily be copied for researchers under the 'fair dealing' provisions of copyright law, but digital rights management systems may prevent this. Avoid using DRM unless it is absolutely necessary.

Privacy

Your digital archive is likely to contain personal data about hundreds of other individuals. Many countries have legislation like the UK's *Data Protection Act (DPA)* which restricts what can be done with personal data about living people. Although the *DPA* does not apply to personal archives while they remain in the creator's possession, it comes into force once custody is transferred to a public repository. You might give some thought to the kind of personal data in your archive, and try and ensure that you act fairly and responsibly in your treatment of other people's data. It is helpful for digital archivists to know which sections of your archive are most likely to contain sensitive information, so they can determine how this material is managed in the repository, and how and when it might be made accessible to researchers in the future.

1 KeePass Password Safe. URL: <http://sourceforge.net/projects/keepass/>
2 Creative Commons, *Creative Commons website.* URL: <http://creativecommons.org/>

9. Keep up to date

Technological changes are rapid and new technologies are constantly appearing. Interoperability with others and the threat of hardware and software obsolescence mean that you must constantly evolve your digital environment, but do think critically about the impact of these new developments before signing up. What effect will they have on your ability to use your personal archive now and in the future? Will you need to change some of your working practices to safeguard your digital materials from new threats? Keep in touch with your digital archivist who will be able to help you assess new technologies, and offer advice about file format, media, software and hardware migration.

10. Handling legacy digital files

You might find yourself dealing with legacy digital files at one time or another - perhaps those of a family member, a predecessor at work, or your own materials, long-abandoned after a software upgrade. These can be in older, unfamiliar, formats, or it may simply be difficult to evaluate their content.

Dealing with older hardware/media

Best to avoid this problem by maintaining your archive! Older hardware and media can be fragile; you may have a limited number of attempts in which you can read and copy data to new media because the process of reading the disk could cause further deterioration. It can be difficult to obtain the necessary drives (in working order) or cables to transfer data. If you do have digital files stuck on older hardware and media, talk to your digital archivist who may be able to help.

Dealing with unfamiliar formats

You need to be able to read and retrieve information from any legacy records you inherit. Your first task should be to identify what formats you are dealing with. There are online registries you can search, to identify formats and applications that can read them. Some formats may be so outdated that alternative operating systems and hardware are also required. Talk to your digital archivist who can provide information on what is needed to access the files and how they may be migrated to more appropriate formats.

Appraising legacy files

When revisiting files you worked with a long time ago, or browsing those of another, it can be tricky to tell what is worth keeping at first glance. You should conduct an initial survey of the material to form an overall impression. This doesn't necessarily entail opening and reading every record; an initial assessment might involve opening a few files in each folder to assess whether the folder title accurately reflects its contents, and an assessment of the likely significance of the material. File names, dates, author and correspondent names can be useful clues. This survey should help you to identify low value material which can definitely be deleted, material which may have short- or medium-term use, and material with long-term personal or research value.

11. Ask digital archivists for advice

Don't just rely on generic guidelines; seek advice from digital archivists and think about where you might deposit your archive in the future!

Eleven top tips for preserving your personal data

	ACTION	KEY INFORMATION	FREQUENCY
1	Name and file appropriately	✔ Develop meaningful and concise filenaming conventions. ✔ Establish a version control system. ✔ Make your files self-documenting.	Ongoing
2	Manage your emails	✔ Select your email client and webmail service carefully. ✔ Follow guidelines on managing your emails effectively.	Ongoing
3	Select suitable formats and software	✔ Use formats that are open, published, standards supported by multiple applications. ✔ Use applications that enable you to use these open formats.	Ongoing
4	Back up files	✔ Decide what should be backed up. ✔ Design a simple backup routine. ✔ Make copies on removable media. ✔ Store a copy offsite. ✔ If online backup/synchronisation services appeal, decide which to use carefully.	Weekly
5	Look after your hardware and media	✔ Replace your hardware before it fails. ✔ Keep hardware/media clean and cool. ✔ Treat removable media with care. ✔ Invest in an Uninterruptible Power Supply.	Ongoing 5 year hardware replacement cycle
6	Administer your system	✔ Ensure files are backed up before updating hardware and software. ✔ Ensure anti-virus software is installed and updated regularly. ✔ Beware of badware.	Ongoing
7	Consider using passwords and encryption devices	✔ Use passwords or encryption devices to protect data on laptops and removable media. ✔ Consider using a password safe to collate data about all your passwords and encryption keys.	At point of record creation – review regularly
8	Be aware of intellectual property and privacy	✔ Respect the intellectual property of others. ✔ Look after your own and others' privacy.	Ongoing
9	Keep up to date	✔ Keep in contact with digital archivists who can update you on developments in digital preservation. ✔ Stay aware of technical trends; evolve your digital environment but be aware of potential effects on your archive.	Ongoing
10	Handling legacy digital files	✔ Ensure records are readable and data is accessible. ✔ Undertake background research and conduct a record survey. ✔ Consult a digital archivist for advice on difficult material	Case by case as needed
11	Ask digital archivists for advice	✔ Don't just rely on generic guidelines; seek advice from digital archivists. ✔ Think about where you might deposit your archive in the future.	As required

Appendix C: Paradigm records survey

Dear Paradigm participant,

Prior to the first visit of the project staff it might be useful for you to think about what digital and paper records are routinely created in your office. We appreciate that you are very busy and therefore this is by no means compulsory. Rather these questions should be seen as a prompt sheet, encouraging you to think about the ways in which records are created, used and stored in your office.

It might be useful to clarify what we mean by a 'record'. A record is that which is created and kept as evidence of individual functions, activities and transactions. It can be in any format whether paper, photographic material, audio tape, maps, or increasingly, in the form of a digital file or object. To be considered evidence a record must possess content, structure and context and be part of a record keeping system. The Paradigm project is particularly looking at procedures for acquiring, managing and preserving records which are in a digital format. For more information about the project, visit <http://www.paradigm.ac.uk>.

What does the office do?

What are the main functions and activities of a MP's London office? What kinds of tasks does the office routinely undertake?

What is the annual routine of the office? When is the office busy/quiet? Are there any events which generate many records?

Who creates the records?

How many members of staff are employed?

What are their key roles?

Record locations: where do you keep paper and digital records?

Where do staff store their digital and/or paper files?

Are records also created at a UK office or elsewhere?

Are records duplicated elsewhere?

How many members of staff are employed at the UK office? What are their key roles?

Does the MP also have further digital records on laptops or PCs at home?

Record types

What types of digital records are used in this office? e.g. word-processed documents, presentations, spreadsheets, databases, webpages, images, PDF, etc.

Roughly how much (in MB, GB) of each record type exists?

Are records created in both paper and digital formats? Are some in both formats? If so which is the master?

What kinds of records does the office create? e.g. speeches, correspondence, newsletters, memos, diaries, etc.

Is most of the correspondence of a routine standardised nature? What kind of topics and correspondents does it contain?

Record keeping systems: how are records maintained and managed through time

Are records kept centrally on a server or does each member of staff manage their own records on their local PC? Are some records kept locally and others centrally?

Is storage space for digital material ever a problem? Are limits imposed?

Are records routinely destroyed? Are there retention schedules which specify how long particular record types should be retained?

Is there an electronic records management system, or electronic document management system, in place?

Web pages:

How often are the web pages updated?

Are copies of previous versions kept?

Who is in charge of the website?

Are there any guidelines or policies in respect of the website?

Email:

How are personal emails organised? e.g. moved into email folders, saved to general folders alongside documents?

Are there any guidelines or policies in respect of email?

Are email and traditional correspondence managed together or separately?

Document files:

How are documents organised?

Are digital and paper records managed together?

What kinds of paper records are created? Are any documents purely in paper format? e.g. diaries, address books, etc.?

Can you provide a list of key records created (all formats)?

Are there any guidelines or rules to help manage the creation of records? Is some kind of version control used?

Are there file plans/ file classification schemes?

Document naming – how are documents named? Are they filed digitally in named folders?

What happens to non-current records?

Privacy

Are some record types of a sensitive nature? (e.g. records which would be closed to researchers for some time, records subject to data protection legislation)

Are any of the records encrypted?

Do any of the records require passwords?

Copyright/Intellectual Property

Who owns the copyright of records held at the office? For example, do you have image files from freelance photographers? If so can copyright be traced?

Technical

Are the office computers networked, stand alone or laptops?

What kind of operating systems are used? e.g. Microsoft Windows XP, Linux, MAC OSX

What is the main software used for records creation?

Does your office use any unusual software?

Do computers have USB ports or CD writers which could be used to copy the material?

What technical support is available?

Who is responsible for IT?

Appendix D: Transfer list

TRANSFER LIST

This transfer list is not a legal document. Its purpose is to record details about the material transferred to the archive to ensure that the authenticity of the material can be audited in the future; to collect details, such as usernames and passwords, needed to access the material; to record contextual information which will be used when compiling finding aids; and to record details about the suggested closure period of records series.

Owner details

Name	
Address	
Telephone	
Email	

Paradigm staff details

Name	
Position	
Address	
Telephone	
Email	

Terms of transfer:

The materials detailed in the schedule of transferred material below are transferred under the terms and conditions set out in the Paradigm project deposit agreement.

SCHEDULE OF TRANSFERRED MATERIAL

Media ref. no. *[Ref. no of CD-R or USB stick, e.g. CD-R-1]*	
MD5 checksum(s) *[record values of MD5 checksum(s)]*	

Extent *[In bytes]*	
Technical description *[description of file formats, passwords]*	
Content Description *[Covering dates, subjects, record types, etc.]*	

Media ref. no. *[Ref. no of CD-R or USB stick, e.g. CD-R-1]*	
MD5 checksum(s) *[record values of MD5 checksum(s)]*	
Extent *[In bytes]*	
Technical description *[description of file formats, passwords]*	
Content Description *[Covering dates, subjects, record types, etc.]*	

Restrictions

Please specify any restrictions to access and use
Does the material contain any confidential items or personal data?

Signatures

Signature of owner or of owner's authorised representative	
Name of signatory	
Date	

Signature of archivist	
Name of signatory	
Date	