UK Association for Accessible Formats UKAAF

G004

Security and data protection

Guidance from UKAAF

UK Association for Accessible Formats (UKAAF)

Because format quality matters

Why format quality matters

"When organisations send me information in formats that I can read myself it allows me to be independent, feel informed and appreciated - just like every other customer."
End-user

"Producing consistently high quality accessible formats helps us to maintain our reputation, to gain new customers and to retain existing ones."
Transcription agency

"We are committed to ensuring that our customers with print disabilities receive the same information, of the same quality, as everyone else."
Service provider

Who is this guidance for?

This guidance from the UK Association for Accessible Formats (UKAAF) is primarily aimed at individual and organisational transcribers of accessible formats.

The guidance includes information on:

- Personnel
- Premises
- Information
- Equipment

Disclaimer

This guidance may include references to external websites, services or products for which UKAAF accepts no responsibility. This information is given without any representation or endorsement of those websites, services or products.

Contents

1 Introduction 5
2 About UKAAF 6
3 Definition of print disability 7
4 Developing security and data protection procedures 7
5 Personnel 7
6 Premises 9
7 Administration 10
8 Computers and networks 11
9 Where to get further help 14
10 Additional resources 15
11 Your feedback is welcome 15

1 Introduction

By obtaining these guidelines you are demonstrating your commitment to helping people with a print disability to read your materials if they find reading standard print materials difficult or impossible.

This guidance concentrates specifically on materials suitable for blind and partially sighted people - such as large print, audio, braille and electronic file formats. However, others with a print disability, for example with dyslexia or motor-difficulties, may also find such materials necessary.

The provision of accessible information is a key requirement of the Equality Act which service providers must follow, but good customer service and business practice includes communicating with your customers and staff in ways which meet their reading needs. By providing accessible format materials, you not only demonstrate your commitment to equality and inclusion, but also increase your reach and customer base. It therefore makes good business sense.

This guidance will help you and your organisation to incorporate good practice into your business and provide good quality accessible format materials in a timely and appropriate way.

Note: This guidance contains advice on security measures that transcribers of accessible formats can use to protect the information they handle on behalf of their customers.

The nature of the transcription industry means that much of the information provided in accessible formats is important and personal. It is essential, with the rise in identity theft and most importantly for the privacy of the individual that transcribers take

their position of privilege in handling confidential or personal data seriously and apply robust security and data control measures.

This guidance will help you and your organisation ensure that the information you handle as part of the transcription process is secure.

2 About UKAAF

The UK Association for Accessible Formats (UKAAF) is the industry association whose mission is to set standards for accessible formats that meet end-user needs through:

- development, delivery and promotion of codes, standards, and best practice for the production and provision of accessible formats
- consultation and collaboration with transcribers, service providers and users of accessible formats.

Members of UKAAF include organisations and individuals with an interest in the provision of quality accessible formats, such as service providers, transcribers, educators, researchers, print services, publishers, and end-users.

Through its leadership and representation, standards-setting, and by fostering a spirit of cooperation between members, UKAAF ensures that the needs and requirements of end-users are understood by service providers and transcribers to help improve the quality of accessible formats.

Please see the section on "Where to get further help" towards the end of this document for more information about the benefits of being a member of UKAAF.

3 Definition of print disability

A print-disabled person is anyone for whom a visual, cognitive, or physical disability hinders the ability to read print. This includes all visual impairments, dyslexia, and any physical disabilities that prevent the handling of a physical copy of a print publication. Source: Copyright Licensing Agency Print Disability Licensing Scheme, Guidelines for Licensees 2010.

4 Developing security and data protection procedures

The first step in implementing appropriate procedures is to develop and publish a security policy. While you are drafting your policy, you should consider the nature of the material you handle and identify those measures and processes that would be appropriate. It may also be useful to share this policy with the commissioner of the confidential material. This means that the commissioner has been given full transparency and can make informed decisions about the type of material that they are happy for you to handle on their behalf.

Even where the type of material that you have been asked to transcribe isn't particularly sensitive or confidential, you and your colleagues should treat any material that belongs to another organisation, or another individual, with respect.

5 Personnel

Even where your organisation employs only one or two members of staff, it is good practice to manage employees as if it were a larger organisation employing many people or teams.

The most basic personal identity check you should make is to obtain references for the people you employ and keep a copy of

their ID on file. This information should be stored securely in a personnel file that contains all the paperwork relating to their employment with you. It should start with their application to join your organisation, their ID and their contract of employment. It should then go on to hold any other communications you have with the individual about their performance or employment, including regular performance review notes.

Further steps that you may need to consider for managing your staff might include restricting access to some materials, especially at the start of their employment, more robust and formal identification processes, and confidentiality agreements that outline any confidential work that they may be asked to do. The confidentiality agreement should form part of their contract of employment with you. The extent to which you would implement any of these measures will depend on the material that your organisation handles and the expectations and processes of your customers.

For some confidential work, you may need to carry out full CRB or police checks on your staff. This will be a requirement agreed with the commissioner at the beginning of a contract. You should also ensure that any volunteers you use for any confidential work are subject to the same checks as your paid staff.

The final measure in implementing your security and data control procedures is training. Training must be thorough and regular, and any issues arising from it must feedback into the future development of your procedures. You should encourage your colleagues to take responsibility for the resilience of your systems, and to be constantly mindful of improvements that could be made.

6 Premises

The security of data begins with the security of the premises in which it is handled. If your transcription premises are an office in a large building over which you have no control, then you should apply as many of the following principles to the area over which you do have control as possible. You should also then consider whether it is appropriate for you to handle confidential material on behalf of external customers.

You should always use common sense in applying these principles. For instance, where the confidential material that you handle belongs to the owner of the building in which you work, such as exam materials belonging to the school in which you work, then you should be guided by that institution on how to handle the material securely.

Where you handle confidential material on behalf of external customers, there are some basic measures that you should apply to your premises.

The office space in which you work should be lockable, and access must be controlled. Where the offices are serviced (such as by a cleaning company), you should have confidentiality agreements with any individuals that need access to your offices.

Access to your office space should be controlled, either by electronic device, or by keys. You should consider whether all of your employees need to hold keys, or other means of access, or whether it should be restricted. Where keys or other means of access have been issued, there must be a record of those and it is advisable to have a regular check that none have been lost. If access is through a keypad, remember to change the code on a regular basis and especially when members of staff leave your organisation.

Visitors should not be able to gain access to your office space. Your staff should be trained in how to handle visitors, including making sure there is a record of their visit and escorting them at all times. You should also consider asking all visitors to sign a confidentiality agreement. This reinforces the sensitivity of the material you handle and makes clear their responsibilities while visiting your premises.

You should also provide an appropriate amount and type of lockable storage in your office space. Once again, it is useful to number the keys that have been issued and for access to the keys to be controlled.

One further measure that you may consider appropriate is to protect your office space with CCTV. This may be more practical and easier to implement if you are not in a shared office space, but for some levels of confidential material, it may be a requirement from your customer. Where you do choose to install CCTV, you should ensure that you backup the CCTV and keep the images for a defined length of time. A CCTV system does not need to be expensive; there are several cost-effective systems available from many DIY stores.

7 Administration

A well-managed transcription process involves several administrative elements including documentation, record-keeping and data control. This is covered in more detail in UKAAF's guidance on "Quality control" (G005).

The level of data control applied to a transcription process will depend on the data in the document. It will also depend heavily on the commissioner being clear on the level of confidentiality that must be applied to a document. If you are not sure whether a

document is confidential, it is advisable to check with the commissioner before you start the transcription process.

However, as a minimum, it is advisable to treat any document that includes a name and address as confidential. For documents that don't include a name and address, the level of confidentiality of each document will need to be agreed with the commissioner.

During transcription work on confidential material, its storage and its identification as "confidential" are very important. Material for transcription that is confidential should be easily identifiable. You may choose to have folders of a particular colour or shape for confidential work.

There should be strict controls on how the material is handled when it is being transcribed and moved around your office space. Your employees must be trained to only take work out of its locked storage when it is to be transcribed and to not leave confidential material unattended on their desk during the process. There should also be a controlled method of transporting material around your office space and a defined process for handing material over to another colleague.

The final step in the data control of confidential material is its disposal. The minimum level of disposal for confidential material is for it to be destroyed in a cross shredder. Where your organisation regularly deals with both confidential and non-confidential material, it may be advisable for you and your employees to treat all waste as confidential.

8 Computers and networks

The issue of protecting electronic data and networks can be difficult for smaller organisations without access to good IT

advisors. However, there are some basic steps that any organisation can put in place.

All PCs and servers must be protected with current anti-virus software. It is also preferable if this software updates automatically. You should also update all other software when updates are available, as these will often include security enhancements.

Your employees should each have their own, unique username and password, and should not allow other colleagues to access a PC using their details. This will allow for an audit trail of access to networks and files if you have auditing software installed. You may also want PCs set to automatically time-out after a certain amount of inactivity.

Unique usernames and passwords will also allow you to restrict access to parts of your network to certain individuals. This may be helpful when you have appointed a new employee and you want to restrict their access to your confidential transcription work.

If you have a server that controls your network, this should be stored in a lockable cabinet or space. Access to this cabinet or space should be controlled and restricted to senior colleagues. You may need to consider how to strike a balance between restricting access to your server and networks, and ensuring that there is ample capability to manage your transcription work.

You may also need to consider how to transfer electronic files that contain sensitive data. There is a wide range of firewalls, File Transfer Protocols (FTP), Secure File Transfer Protocols (SFTP) and encryption available to protect data that you need to transfer in and out of your premises. The level of protection that you need will often be determined by the commissioner, but you may choose to have some level of protection regardless.

A firewall sits between your network, or your computers, and the internet. It protects your network by managing the flow of information and restricting access. A firewall can be a standalone unit, costing in the region of £300 to £500, or a software firewall costing between £1,500 and £7,000. You will need to investigate the system and price that suits your business.

FTP is a method of allowing the transfer of large files by uploading and downloading the data, instead of sending files via email. However, there is no security to this process. If you need to transfer large files securely, you will need to establish an SFTP. There are commercial solutions, as well as open source versions for this. Often, the commercial options will be better supported, but the open source versions will serve the same function.

Encryption is a process that makes a file or email accessible only to an authorised user. Where you are encrypting a file to transfer to another user, you will need to have exchanged personal encryption keys to make sure that the recipient can access the file. You can also encrypt whole hard disks to protect them if they are taken from your premises. To encrypt data, you can buy commercial software that is fully supported or use free open source solutions. Open source software may be less user-friendly, but will achieve the same results as commercial software.

As with your administration procedures, the final issue for managing the security of your networks is disposal of data and hardware. Your policy should include information on how long you retain files and how files are destroyed. Deleting an electronic file from a computer does not destroy the data contained in the file, so you will need to have software that overwrites files. You must also have a record of any equipment that you dispose of and assurances that this has been done thoroughly.

It is advisable that computers and computer systems that have been used for secure data storage or production, should not be sold or donated to charity. When finished with, the machinery should be made unusable by anyone else. There are companies that do this for money, or there is software that you can purchase that will completely shred the information electronically.

9 Where to get further help

UKAAF assists businesses and organisations by advising how to meet the needs of customers and clients with print disabilities; providing guidance on how to source and provide quality accessible formats like large print, audio, braille, electronic file formats and Easy Read; and helping you to understand your responsibilities as a service provider.

Through our website and magazine, members will also gain access to:

- findings from public consultations and end-user research
- research and innovation in accessible formats
- information on suppliers of transcription services
- guidance and advice on standards for accessible formats
- opportunities to review and help to develop standards and guidance.

In addition to supporting service providers and transcribers, UKAAF also represents people with print disabilities. We believe that because format quality matters, end-users should have genuine input into the development of standards for accessible information. By collecting and sharing users’ views with service providers and transcribers we can help them to deliver a quality service which meets users' needs.

UKAAF has a User Advisory Group (UAG) so we can include blind and partially sighted people and others with print disabilities in ongoing research and consultation on key accessible format issues.

There are many benefits of being a member of UKAAF, not least to demonstrate your commitment to quality accessible formats. For more information visit us at www.ukaaf.org.

10 Additional resources

The Information Commissioner's Office (ICO) has information on your legal obligations under the Data Protection Act www.ico.gov.uk

The Business Link website has a vast amount of information for organisations on developing policies and procedures, including information security policies www.businesslink.gov.uk

The British Standards Institution (BSI) has information on data protection training and BS10012, a standard for managing personal information www.bsigroup.co.uk

The IT governance site has information, advice and resources on information security www.itgovernance.co.uk

11 Your feedback is welcome

We would welcome your views on this guidance, any suggestions for additions, or case studies of how this guidance has helped you. You might like to share your experience in an article in our magazine 'Format Matters'.

You can phone, email or write to us - our details are at the back, or use the feedback form on our website www.ukaaf.org.

If you find UKAAF's guidance valuable, please encourage others to join by visiting our website.

Document reference information

Citation guidance	Security and data protection: Guidance from UKAAF (2012) UK Association for Accessible Formats. Ref: G004
Document title	Security and data protection: Guidance from UKAAF
Publisher	UK Association for Accessible Formats (UKAAF)
Document ref	G004
Version number	1.0
Publication date	June 2012
Document purpose	Good practice guidance for transcribers
Primary contributors	Sheila Armstrong, Sarah Home, Alan Matthews, Marion Ripley, Sharon Williams
Board approval	June 2012
Acknowledgements	With thanks to all our reviewers for their valuable comments
Superseded documents	N/A
Template version	1.0

Notes

Notes

UK Association for Accessible Formats (UKAAF)

Contact details

UKAAF
PO Box 127
Cwmbrân
NP44 9BQ

Tel: 0845 60 85223
Fax: 0845 60 85224
Email: enquiries@ukaaf.org
Web: www.ukaaf.org

Registered address

UKAAF
c/o Pia
Victoria Street
Cwmbrân
NP44 3YT

President: Lord Low of Dalston CBE
Registered charity number: 1126966
Registered as a company in England and Wales number: 6748900