Staff Data Protection Guidance Document

How to look after personal information

As and when

- Ensure that the starters and leavers checklist is complete (e.g. setting up and removing access for sensitive information)
- Ensure that personal information is only shared with those who need access to it - link to shared folders rather than email around personal data
- Only pass on people's personal information to others (e.g. external contacts) with their permission
- Don't write down people's card details, or if you have a credit card / direct debit form ensure it is safely stored away and ensure it is cross cut shredded
- Review your own and department processes - do you need to keep personal info in a spreadsheet and is access to it limited and securely kept? Or can it live in Spektrix instead?

Monthly detox

- Delete your computer download folder
- Delete your Outlook deleted folder items
- Review your folders and who has permissions to access them, update if needed
- Check you don't have personal information in hard copy that is no longer needed - ensure it is securely shredded, not just put in recycling
- Ensure sensitive and personal information has restricted access and that you update passwords every 3 months (IT systems to automate this as much as possible - general manager to take responsibility)

6 month detox

- Delete personal information of non-successful applicant data after 6 months and delete people after a year (add application and interview forms have this information)
- Delete core staff details who have left in perpetuity (unless there is a legimate interest to stay in touch for future work)
- Alert General Manager if any of your personal details have changed (address, mobile phone number, emergency contact)
- If you want to keep someone’s data for longer than time periods above, ask for their consent and make sure end date info is added to their details and updated / deleted at that point
- Annual clean-up
- Destroy any copies of direct debit forms on shared drive or hard copy
- Destroy any hard copy contact sheets
- Minimise access to contact information of past staff / shows if your department no longer requires immediate access to it

General Policy

- Think about the risks of sharing people's personal information - ensure you minise the risks and that you have permission / legimitate reason to use or share their information
- Only keep personal data if it necessary and useful
- Only ask for information that is relevant for what you need

- You can feel reassured that you don't need to delete the information of people you are friends with, or who may come back in the future, such as creative team members
- Staff sharing email inboxes should be set up with their our network login so that activity is audited.
- Ensure you log off if you are not at your computer, ensure your phone locks after 1 minute, ensure shared email addresses cannot access a shared inbox on phone
- Working from home
- Have a working from home induction: talk to HR to set parameters of working from home, ensure that you have considered and that working from home parameters are set
- Use webmail to access emails
- Consider the risks around working remotely and level of security needed for particular data (i.e. children's information)
- Have own profile on home computer (ie. do not share with a partner)
- Remote in on the shared drive
- Clear your downloads folder on your phone and home computer after downloading work materials - do this on the sanme day as worked so they don't get saved to back ups
- Password protect files
- Consider which carries the greater risk - emailing yourself information (which could be forwarded indefinitely), or carrying a hard copy (which could be left on a train)
- Ensure that your computer has up to date security in place particularly if accessing the internet, only use secure WiFi rather than public / company WiFi

Top five tips from the ICO

Here are our top five of data protection tips for small and medium sized charities and third sector organisations:

1. Tell people what you are doing with their data

People should know what you are doing with their information and who it will be shared with. This is a legal requirement (as well as established best practice) so it is important you are open and honest with people about how their data will be used.

2. Make sure your staff are adequately trained

New employees must receive data protection training to explain how they should store and handle personal information. Refresher training should be provided at regular intervals for existing staff.

3. Use strong passwords

There is no point protecting the personal information you hold with a password if that password is easy to guess. All passwords should contain upper and lower case letters, a number and ideally a symbol. This will help to keep your information secure from would-be thieves.

4. Encrypt all portable devices

Make sure all portable devices – such as memory sticks and laptops – used to store personal information are encrypted.

5. Only keep people’s information for as long as necessary

Make sure your organisation has established retention periods in place and set up a process for deleting personal information once it is no longer required.

Computer security

- Install a firewall and virus-checking on your computers.
- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Email security

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Fax security

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.

- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

Other security measures

- Shred all your confidential paper waste.
- Check the physical security of your premises.
- Staff training and security

Train your staff:

- so they know what is expected of them;
- to be wary of people who may try to trick them into giving out personal details;
- so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Starters checklist

- Move application form from Recruitment folder to Personnel
- File interview notes in hard copy Personnel file
- Employee to fill in starter form
- Employee to fill in Emergency Action form
- Equal Opps and Emergency Action form to Stage Door for processing
- GM to complete starter form, save a copy and pass to Finance
- Sign and return contract
- Contract - needs to be in line with current HR best practice, your employee file will be kept for five years after your last day here.'
- Send policy docs by email to read
- Written email confirmation that the new employee has read and understood the policy docs sent to them
- Send staff handbook by email
- Set up a profile and email account
- Fire safety and building tour
- Office induction: phones
- Office induction: server docs, email, calendars
- Office induction: photocopier / scanner / printer
- Add staff information to Spektrix with 'staff' tag

- Add staff to staff phone list
- Add staff to emergency contacts spreadsheet
- Add staff to any relevant WhatsApp groups
- Ensure Spektrix settings are correct and access is limited

Leavers checklist

- Exit interview: A chance to ask them privately if there is anyone in the company who they would rather not have their mobile / personal email
- Divert / out of office message on emails 'This person has now left the Unicorn. Your email has been automatically forwarded to X.'
- Change their profile password
- Change their webmail password
- Delete their profile
- Update passwords
- Update door codes
- Ask for return of keys   Update key holder sheet
- Final payroll - P45 generated at last payrun
- Ask staff if they want to continue to receive Unicorn invites for the next year or so and if they want to receive Unicorn News - ask for a new work / personal email address if so
- Update their Spektrix account info according to answers to above
- Update staff phone list
- Update emergency contacts spreadsheet
- Remove staff from any WhatsApp groups