General Resources & Information

- ICO Information Top Tips - https://ico.org.uk/media/for-organisations/documents/1568/information_rights_top_tips.pdf
- ICO Guidelines for Data Protection - https://ico.org.uk/for-organisations/guide-to-data-protection/
- Preparing for GDPR (12 top tips) - https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- ICO Data Protection Self-Assessment Toolkit - https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment-toolkit/
- Data Protection Network - https://www.dpnetwork.org.uk/ (its free to sign up)
- ICO Helpline (for small organisations under 250 staff) - 0303 123 1113 and select option 4 to be diverted to staff who can offer support

Specific Information

- NHS Digital - https://digital.nhs.uk/data-security-information-governance
- Impacts on Fundraising Activity - https://www.institute-of-fundraising.org.uk/guidance/research/get-ready-for-gdpr/spotlight-series/
- Parish Resources (Faith Based Perspective) - http://www.parishresources.org.uk/gdpr/
- Scouting Organisations - https://members.scouts.org.uk/supportresources/search/?cat=55,888
- Children and GDPR (ICO Consultation Document) - https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/children-and-the-gdpr-guidance/

			Where to find further support	Your Notes
1.	Do you know exactly what information you hold, why and who you share it with?	Yes / No / Not Sure	**National Archives - guidance** http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/find-out-what-information-you-have/ **ICO Lawful Basis Guidance Tool** - https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/lawful-basis-interactive-guidance-tool/ **Data Audit** Conducting a data audit using the template provided or a simplified version will help you identify what data you hot, why, your conditions for processing and who you share it with. As well as how long you keep it and how it's disposed of.	
2.	Do you have a data protection / information governance policy?	Yes / No / Not Sure	**Guide to writing a Data Protection Policy (NCVO members only)** https://knowhownonprofit.org/tools-resources/hr-policies/data-protection **Sample Data Protection Policies** https://iapp.org/resources/article/sample-data-protection-policy-template-2/ http://www.harrisvs.org.uk/home_htm_files/Data%20Protection%20Policy%20Model%202013.doc	

			Sample policies cont… https://www.valonline.org.uk/sites/www.valonline.org.uk/files/model_data_protection_policy_2015_0.doc	
3.	Does your data protection / Information Governance Policy link to other policies and procedures in your organisation?	Yes / No / Not Sure	Good information governance links to a number of policies and documents within your organisation including IT usage, mobile phone policies, confidential policies, business continuity, staff handbooks etc. You may need to refresh these to include elements of data protection.	
4.	Does your IT system meet “cyber essentials”?	Yes / No / Not Sure	**Cyber Essentials** Complete the checklist given on the course or complete is online at https://www.cyberaware.gov.uk/cyberessentials/#questionnaire **Cyber Aware (support resources)** https://www.cyberaware.gov.uk/ **National Cyber Security Centre Small Charities Guide** - https://www.ncsc.gov.uk/charity	

5.	Do you have a named lead for data protection?	Yes / No / Not Sure	See preparing for GDPR resource above:- You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. Often this role sit alongside other compliance issues including finance and HR. Most VCSE organisations do not a formal Data Protection Officer designated under GDPR (large scale processing or a recognised public body). Information on this role can be found from NHS digital - http://bit.ly/2FbkBhj	
6.	Is information governance / data protection discussed at a board or committee level?	Yes / No / Not Sure	Information Governance and Data Protection is a compliance issues in the same way as finance or health and safety. Policies, incidents and risks should all be discussed and minuted at this level as part of good governance and help you demonstrate the processes you've done. You may find it useful to do an information governance risk register or to incorporate this into your organisation risk register to support this.(see attached template)	

6.	Do you need to register with the ICO?	Yes / No / Not Sure	**ICO Current Registration Self-Assessment Tool** (a free 5 minute online tool to assess if you need to register) https://ico.org.uk/for-organisations/register/self-assessment/ **ICO Guide for Controllers from May 2018 (Feb 18)** https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf	
7.	Have key staff or volunteers attended training?	Yes / No / Not Sure	For key staff this may be formal training such as today but this will depend on their role. Think about how data protection is covered in inductions and if everyone is aware of your policies. Ensure any training given is recorded either through HR files or minutes of team meetings, 1:1 etc	
8.	Do you have appropriate privacy notices in place and available	Yes / No / Not Sure	**The Fundraising Regulator – Checklist of things to consider** https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/ChecklistFinal.pdf **ICO Privacy Access Guidance** https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/	
9.	Do you ensure that people have consent for their information to be used? Does this need reviewing?	Yes / No / Not Sure		

	Cont….		**ICO Guidance on Consent** https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/ **ICO Presentation on Fundraising and Regulatory Compliance for Charities** https://ico.org.uk/media/about-the-ico/events-and-webinars/2013443/frcc2017-presentation-opening-the-box-fundraising-and-regulatory-compliance.pdf **DPN - Legitimate Interests Guidance** https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/ **Young People Advisory Service (example users poster – how we keep notes on you)** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/Voluntary%20Sector%20%20Exemplar_YPAS_How%20we%20keep%20notes%20about%20you.doc **Parish Resources (sample notice)** http://www.parishresources.org.uk/wp-content/uploads/Sample-Privacy-Notice_18.docx Make sure you record somewhere what consent was given, when and how – this may be part of a database, CRM system or membership record.	

10.	Do you ensure the data you hold is accurate and up to date?	Yes / No / Not Sure	**Shred-it Guide to Data Retention** https://www.shredit.co.uk/getmedia/79634da2-8885-461f-9c6e-195c617a0562/Doc_Retention_Guide_UK_E.aspx?ext=.pdf **ICO Guidance on Data Retention** https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/ **Lambeth Palace Library (Church of England) record keeping guides** http://www.lambethpalacelibrary.org/content/recordsmanagement **HR records standard retention periods** (for guidance only) - https://www.orsgroup.com/department-solutions/human-resources/statutory-retention-periods	
11.	Do you have a process in place if people want to access their own personal data?	Yes / No / Not Sure	**ICO Subject Access Request Checklist** – A 2 minute tool to support organisations dealing with a request https://ico.org.uk/for-organisations/subject-access-request-checklist/	

	Cont….		**ICO Code of Practise (the full document)** https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf#page=14	
12.	Do you have a process in place to support information sharing?	Yes / No / Not Sure	**Example information sharing policy** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/Voluntary%20Sector%20%20Exemplar_YPAS_Information%20Sharing%20Policy.doc **ICO Data Sharing Code of Practise** https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf **ICO Data Sharing Checklist** https://ico.org.uk/media/for-organisations/documents/1067/data_sharing_checklists.pdf	
13.	Do you have a process in place to transport personal information securely?	Yes / No / Not Sure	**Encrypted Email** https://protonmail.com/ - A free EU based encrypted email system **Mass Email / Newsletter Programmes -** https://moosend.com/ (UK based) https://emailoctopus.com (UK based, promised compliance from May 18)	

	Cont….		**Zip Drives – free compression software** http://www.7-zip.org/ http://www.peazip.org/ https://www.zipware.org/ https://www.ashampoo.com/en/usd/pin/0192/system-software/zip-free **Dropbox** – cloud storage moving to comply with GDPR https://www.dropbox.com/help/security/general-data-protection-regulation Other cloud providers are doing similar work but you need to check to ensure compliance!	
14.	Do you have a process to dispose of data that you no longer require?	Yes / No / Not Sure	How long you keep data depends on its purpose. Your retention and disposal policy will depend on statutory requirements (e.g. finance, safeguarding etc.), contractual (e.g. how long the commissioner or funder (such as ESF) want you to keep it) or business case (how long you need it). The key thing is justifying why you're keeping it and recording it. It could be an appendix to your data protection policy rather than a whole separate document. **ICO Guidance for Deleting Personal Information** https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf	

	Cont…..		**ICO IT Asset Disposal Guidance** https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf **NHS England Bite Sized Guide to Media Disposal** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/Bite-sized%20GPG_Media%20Disposal.doc	
15.	Do you ensure that all the data you hold is held securely?	Yes / No / Not Sure	**Get Safe Online –** General Advice and Support re Cyber Security https://www.getsafeonline.org/ **ICO Guide to Encryption** https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/ **ICO Practical Guide to IT Security** https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf **Guide to Print Security (Multipurpose printers)** https://www.canon-europe.com/images/ICO%20Canon%20Practical%20Guide%20to%20Print%20Security_tcm13-1000094.pdf	

	Cont….		**Government Guide to Cyber Security** https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf	
16.	Do you have processes in place in case information is lost, stolen or accessed inappropriately?	Yes / No / Not Sure	Try to record and act on any near misses or potential breaches. Human error and mistakes happen but you may wish to include not reporting a breach within your staff / volunteer handback as a potential disciplinary matter. **ICO Guidance on Breach Management** https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf **ICO Guidance on Reporting a Breach** https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf **ICO Breach Notification Form** https://ico.org.uk/media/for-organisations/documents/2666/security_breach_notification_form.doc **Example IG Incident Reporting Form** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/Voluntary%20Sector%20%20Exemplar_YPAS_IG%20Information%20Incident%20Reporting%20Form.doc	

17.	Do you consider information governance and data protection within your project and programmes	Yes / No / Not Sure	Considering the data implications of a project at the start of a project is good practise and helps avoid any pitfalls later on. Privacy Impact Assessments can help both on specific programmes as well as more broadly in terms of identifying risk to your organisation. **ICO Data Protection Impact Assessments (DPIAs) guidance** - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/ **ICO Privacy Impact Assessment Code of Practise** https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf	