				Risk and priority	Target date	Activity	Records	Dependencies	Progress
	Lawfulness, fairness and transparency								
1	Information audit, mapping data flows undertaken	Identify the data that is processed, and how it flows into, through and out of your business. This includes flow from one location to another within the organisation. Identify any risks. The ICO has issued a data flow mapping and information sharing template.	*organise and record an information audit across your business or within particular business areas to identify the data that you process and how it flows into, through and out of your business;– *identify and document any risks you have found, for example in a risk register	high	25-May	Identify and record personal data held	ROPA (Record of processi	HR and payroll data is processed by the Force.	Complete
2	Personal data held is documented	If you have less than 250 employees then you must keep records of any processing activities that: * are not occasional; * could result in a risk to the rights and freedoms of individuals; or * involve the processing of special categories of data or criminal conviction and offence data. If you have over 250 employees, you must record the following information: * name and details of your business (and where applicable, of other controllers, your representative and data protection officer); * purposes of the processing; * description of the categories of individuals and categories of personal data; * categories of recipients of personal data; * where applicable, details of transfers to third countries including documentation of the transfer mechanism safeguards in place; * retention schedules; and * a general description of technical and organisational security measures. You may be required to make these records available to the ICO on request	*maintain records of processing activities detailing what personal data you hold, where it came from, who you share it with and what you do with it. This will vary depending on the size of your business; *consider using an information asset register to do this; and *ensure you have procedures to guide staff on how to manage information you hold	high / medium	25-Sep	*Identify and record personal data held. *record storage methods and security for records held *Review record retention policy and schedule and circulate to staff. *Review DP and Info Security and Info sharing policies and procedures and circulate to staff *write information sharing procedure and create sharing decision log, and circulate to staff (see row 27)	*ROPA (to include storage security) *Record retention policy and schedule *DP, Info security and info sharing policies and procedures	Updated policies may not be complete by 25 May.	Complete
3	Lawful bases for sharing and processing data is documented	Lawful bases need to be identified before you can process personal data and special categories of data. The lawful bases for processing have an effect on individual's rights, e.g. when relying on consent, subjects will have a stronger right to have data deleted. You must let individuals know how you intend to process their personal data, and what your lawful bases are for dointg so, e.g in privacy notices.	*look at the various types of data processing you carry out; *identify your lawful bases for carrying it out; and *document it, for example in your privacy notice(s).	High	public data 25 May Internal data 1 July	Identify and record legal bases. Write individual privacy notices for all types of processing	ROPA Privacy notices	Privacy notices for data processed by Force cannot be completed until data flow information received by Force.	Complete- ongoing need for privacy notices expected.
4	Review undertaken regarding how we ask for and record consent, and how we manage consent.	The GDPR sets a high standard for consent but remember you don't always need consent. You should also assess whether another lawful bases is more appropriate.—Consent means offering people genuine choice and control over how you use their data. You can build trust and enhance your business by using consent properly.—The GDPR builds on the DPA standard of consent in several areas and contains much more detail:—* Keep your consent requests separate from other terms and conditions.—* Consent requires a positive opt-in. Use unticked opt-in boxes or similar active opt-in methods.—* Avoid making consent a precondition of service.—* Be specific and granular. Allow individuals to consent separately to different types of processing wherever appropriate.—* Name your business and any specific third party organisations who will rely on this consent.—* Keep records of what an individual has consented to, including what you told them, and when and how they consented.—* Tell individuals they can withdraw consent at any time and how to do this.— Your obligations don't end when you first get consent. You should continue to review consent as part of your ongoing relationship with individuals, not a one-off compliance box to tick and file away.Keep consent under review, and refresh it if anything changes. You should have a system or process to capture these reviews and record any changes.If your current consent doesn't meet the GDPR's high standards or is poorly documented, you will need to seek fresh GDPR-compliant consent, identify a different lawful basis for your processing (and ensure continued processing is fair), or stop the processing	*Check that consent is the most appropriate lawful bases for processing *Make the request for consent prominent and separate from your terms and conditions *Ask individuals to positively opt in.–Use unticked opt-in boxes or similar active opt-in methods *Use clear, plain language that is easy to understand *Specify why you want the data and what you're going to do with it *Give granular options to allow individuals to consent separately to different types of processing wherever appropriate *Name your business and any specific third party organisations who will rely on this consent *Tell individuals they can withdraw consent at any time and how to do this *Ensure that individuals can refuse to consent without detriment *Don't make consent a precondition of service Keep a record of when and how you got consent from the individual *Keep a record of exactly what they are told at the time *Regularly review consent to check that the relationship, processing and the purposes have not changed*Have processes to refresh consent at appropriate intervals, including any parental consent *Consider using privacy dashboards or other preference management tools as a matter of good practice. *Make it easy for individuals to withdraw their consent at any time and publicise how to do so.*Act on withdrawals of consent as soon as you can. *Don't penalise individuals who wish to withdraw consent. *If current consent don't meet the GDPR's high standards or is poorly documented, your business will need to;–seek fresh GDPR-compliant consent; or–identify a different lawful bases for your processing (and ensure continued processing is fair); or–stop the processing.—	high	25-May	*Identify data processing that requires consent in ROPA *Write consent forms for each, to include all requirements in column D, to include date and method of request fields *Create folders in corporate filing system to store consent forms (by year and name) OR save in associated Pentana record. *Schedule repeating 12 month review of consent for all processing that relies on consent and is ongoing	ROPA Consent forms Consent files in corporate filing system Review of consent process and reminders		Complete
5	Registration	Until May 2018 a registration with the ICO is required. Aftger May 2018, you need to pay the ICO a data protection fee.					Registration record		PCCs not required to register with the ICO.
	Individuals rights								
5	Privacy notices have been provided to individuals	Gives information about what data is collected, why processed and who shared with. This information should be published in a privacy notice on the website, and within any forms and letters sent to individuals The information must be consise, transparent, intelligible and easily accessible	Your privacy notice should:– *let individuals know who you are, why you are processing their data and who you share it with; *be concise and to the point *be easy to understand; *be clearly signposted and easy to access *be written in clear and plain language, particularly if addressed to a child; *free of charge; *include different information depending on whether you obtained the data directly from the individual or not; and– *be reviewed regularly to make sure it remains accurate and up to date	public data - high Internal data - medium	Public privacy notices by 25 May. Internal privacy notices by 1 July	Write privacy notices for all data types and processing	Privacy notices	Ability to write privacy notices for HR data is reliant on information from Force on processing undertaken.	Complete. Ongoing need for privacy notices expected.
6	There is a process to recoginse and respond to individuals requests to access their personal data	Individuals have the right to obtain:–* confirmation that their data is being processed;–* access to their personal data; and–* other supplementary information – this largely corresponds to the information that you should be provided in a privacy notice.–You should provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request:–* is manifestly unfounded or excessive, particularly if it is repetitive, unless you refuse to respond; or–* is for further copies of the same information (that's previously been provided). This does not mean that you can charge for all subsequent access requests.–The fee must be based on the administrative cost of providing the information.–You will have less time to comply with a subject access request under the GDPR. Information must be provided without delay and at least within one calendar month of receipt. You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). –A calendar month ends on the corresponding date of the next month (eg 2 January to 2 February), unless that date does not exist in which case it is the last day of the next month (eg 31 January to 28 February). –This means that the legal deadline will vary from 28 days to 31 days depending on the month. For practical purposes if a consistent number of days is required (eg for a computer system), it may be helpful to adopt a 28-day period to ensure compliance is always within a calendar month.–You must verify the identity of the person making the request, using "reasonable means".–If the request is made electronically, you should provide the information in a commonly used electronic format.–.—	ensure a process is in place to allow you to recognise and respond to any subject access requests within the timescales *include subject access procedures within your data protection policy *provide awareness training to all staff and specialist training to individuals who deal with any requests; and *consider if you can provide remote access to a secure self-service system to provide the information directly to an individual in response to a request (this will not be appropriate for all organisations, but there are some sectors where this may work well).—	high	25-May	*Review and update subject access process on website *Provide training on GDPR for staff that includes subject access requests	Subject access process Training records		Complete. Ongoing need for training.
7	There is a process that ensures the personal data held remains accurate and up to date	Individuals have the right to have personal data rectified if it is inaccurate or incomplete.–You should respond to a request without delay and at least within one month of receipt.–You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). If you have disclosed the personal data to a data processor (third party) you must inform them of the rectification where possible.–You should regularly review the information you process or store to identify when you need to do things like correct inaccurate records. Records management policies, with rules for creating and keeping records (including emails) can help.–Conducting regular data quality reviews of systems and manual records you hold will help to ensure the information continues to be adequate for the purposes of processing (for which it was collected).–You should also ensure that there are regular data quality checks completed to provide assurances on the accuracy of the data being inputted by staff.–If you identify any data accuracy issues, communicate lessons learned to staff through ongoing awareness campaigns and internal training.—	•implement procedures to allow individuals to challenge the accuracy of the information you hold about them and have it corrected if necessary; •have procedures to inform any data processors (third parties) you have disclosed the information to about the rectification where possible; •create records management policies, with rules for creating and keeping records (including emails); •conduct regular data quality reviews of systems and manual records you hold to ensure the information continues to be adequate for the purposes of processing (for which it was collected); •regularly review information to identify when you need to correct inaccurate records, remove irrelevant ones and update out-of-date ones; and •promote and feedback any data quality trends to staff through ongoing awareness campaigns and internal training.	High	25 May	*Write procedure for website (include in generic privacy notice) *Include statement in all other privacy notices *Ensure all staff dealing with personal data are aware of the process, and the need to inform third parties *Review and update records management policy, and guide to the corporate filing system, and record retention policy	Generic and specific privacy notices Record of procedures to staff Records management police Guide to the corporate filing system Record retention policy		Suggest that this will only apply to Staff and volunteer / member / etc personnel records, and newsletter distribution lists where there is ongoing processing. Subject Access process includes information on how to notify us of corrections.
8	There is a process to securely dispose of personal data that is no longer required, or where an individual has asked for it to be erased.	The record retention schedule should be regularly reviewed to ensure it continues to meet business and statutory requirements. Responsibility for retention and disposal should lie with a designated appropriate person. An individual has a right to request erasure for a number of reasons including no longer necessary for original purpose, withdrawal of consent / objection to processing in the absence of a legitimate interest for the processing. You can refulse to comply where personal data is processed for right of fredom of expression, comply with a legal obligation for performance of a public interest tasks or exercise of public duty, public health purposes, archiving purposes in public interest, scientific research, historical research, statistical research, exercise or defence of legal claims.	•have procedures in place which allow individuals to request the deletion or erasure of their information your business holds about them where there is no compelling reason for its continued processing; •have procedures to inform any data processors (third parties) you have shared the information with about the request for erasure; •have procedures to delete information from any back up systems; •implement a written retention policy or schedule to remind you when to dispose of various categories of data, and help you plan for its secure disposal; •regularly review the retention schedule to make sure it continues to meet business and statutory requirements; •assign responsibility for retention and disposal to an appropriate person; •have appropriate methods of destruction in place to prevent disclosure of personal data prior to, during and after disposal; and •if you use third parties to dispose of personal data on your behalf, your contract includes the requirement for them to have	High	25 June	*Include procedure in generic privacy notice on website *Include procedure in specific privacy notices *Update DP policy *Review and update record retention policy and schedules and identify data types where there is a 3rd party processer to notify *undertake a whole office review of data held and weed in accordance with the rention policy and schedules. * Share procedures with staff.	Generic and specific privacy notices Record of procedures to staff Record retention policy and retention schedules DP Policy	Deletion of records from backup systems is dependent on the Force ICT practices.	

9	There is a process to respond to an individual's request to restrict the processing of their personal data	When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in the future.You will be required to restrict the processing of personal data in the following circumstances: * Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data. * Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your businesses legitimate grounds override those of the individual. * When processing is unlawful and the individual opposes erasure and requests restriction instead. * If you no longer need the personal data but the individual requires the data to be retained to allow them to establish, exercise or defend a legal claim. You may need to review procedures to ensure you are able to determine where you may be required to restrict the processing of personal data.If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.You must inform individuals when you decide to lift a restriction on processing	•review your procedures to determine where you may be required to restrict the processing of personal data; •implement a process that will enable individuals to submit a request to you; •have a process to act on an individual's request to block or restrict the processing of their personal data; •have procedures to inform any data processors (third parties) you have shared the information with, if possible; and •inform individuals when you decide to lift a restriction on processing.	High	25-Jun	*Include procedure in generic privacy notice on website *Include procedure in specific privacy notices *Update DP policy *Review and update record retention policy and schedules and identify data types where there is a 3rd party processer to notify *Create a log to record details of who and when a data subject has requested a restriction on their data, and and other relevant details, and activity required. *include a reference in the record retention policy to check the log before deleting information. * Share procedures with staff.	Generic privacy notice Specific privacy notices DP policy Record retention policy Log of data subjects requesting data processing restrictions		Included in data subject access process - published.
10	There is a process to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way without hindrance to usability.	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.–They can receive personal data or move, copy or transfer that data from one business to another in a safe and secure way, without hindrance.–The right to data portability only applies:–* to personal data an individual has provided to a controller;–* where the processing is based on the individual's consent or for the performance of a contract; and–* where the processing is carried out by automated means. Information must be provided without delay and at least within one month of receipt.–You can extend this period by a further two months for complex or numerous requests (in which case the individual must be informed and given an explanation). –You must provide the personal data in a structured, commonly used and machine readable format. Examples of appropriate formats include CSV and XML files. –You must provide the information free of charge.–If the individual requests it, you may be required to transmit the data directly to another business where this is technically feasible.——	•implement a process that will enable individuals to submit a request to you; •have a process to allow you to recognise and respond to any individual requests in line with your legal obligations and statutory timescales; •provide the personal data in a structured, commonly used and machine readable format; •ensure that the medium in which the data is provided has appropriate technical measures in place to protect the data it contains; and •ensure that the medium in which the data is provided allows individuals to move, copy or transfer that data easily from one organisation to another without hindrance.	High	25-May	Include in subject access request procedure Share process with staff	Subject access process Record of sharing with staff		Included in data subject access process - published.
11	There are procedures to handle an individual's objection to the processing of their personal data.	Individuals have the right to object to:–* processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); and–* processing for purposes of scientific/historical research and statistics.–Individuals must have an objection on "grounds relating to his or her particular situation".–However for processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority or for purposes of scientific/historical research and statistics you must stop processing the personal data unless:–* you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or–* the processing is for the establishment, exercise or defence of legal claims.–Individuals also have the right to object to any processing undertaken for the purposes of direct marketing (including profiling). You must stop processing for direct marketing as soon as you receive an objection. There are no exemptions or grounds to refuse.–You must inform individuals of their right to object "at the point of first communication" and clearly lay this out in your privacy notice.–—	•review your processes and privacy notice(s) to ensure they inform individuals of their right to object "at the point of first communication". This information should be displayed or given clearly and separately from any other information; •implement a process that will enable individuals to submit an objection request (this could include an online option); •have processes in place to investigate an individual's objection to the processing of their personal data within the legitimate grounds outlined within the GDPR; and •provide training or raise awareness amongst your staff to ensure they are able to recognise and respond (or know where to refer the request to) to an objection raised by an individual.	High	25-May	*Include procedure in generic privacy notice on website *Include procedure in specific privacy notices *Update DP policy *Review and update record retention policy and schedules and identify data types where there is a 3rd party processer to notify *log objections on Covalent RMS under the DP type for processing. * Share procedures with staff.	Generic privacy notice Specific privacy notices DP policy Record retention policy Log of objections on Covalent Record of sharing with staff		Included in data subject access process - published.
	Accountability and governance								
12	There is an appropriate data protection policy	The GDPR requires you to show how you comply with the principles. –A policy will help you address data protection in a consistent manner and demonstrate accountability under the GDPR. This can be a standalone policy statement or part of a general staff policy. –The policy should clearly set out your approach to data protection together with responsibilities for implementing the policy and monitoring compliance. –The policy should be approved by management, published and communicated to all staff. You should also review and update the policy at planned intervals or when required to ensure it remains relevant.–Your business monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls. ——	You should have a standalone policy statement or general staff policy that •sets out your business's approach to data protection together with responsibilities for implementing the policy and monitoring compliance; •aligns with and covers the measures within this checklist as a minimum; •is approved by management, published and communicated to all staff; and •is reviewed and updated at planned intervals or when required to ensure it remains relevant.	High	25-May	*Review and update DP policy *Schedule in annual reviews of DP policy	DP policy Schedule and record of reviews undertaken (may be on front page of policy)		Complete
13	There are systems to monitor compliance with data protection policies and regularly review the effectiveness of data handling and security controls.	Documenting policies alone is often not enough to provide assurance that staff are adhering to the processes that they cover. You should ensure that you have a process to monitor compliance to data protection and security policies. Measures that are detailed within the policies should be regularly tested to provide assurances as to their continued effectiveness. Responsibility for monitoring compliance with the policy shoudl be independent of the persons implementing the policy, to allow the monitoring to be unbiased. Results of compliance testing shoudl then be reported on a regular basis to senior management.	•establish a process to monitor compliance to the policies; •regularly test the measures that are detailed within the policies to provide assurances that they continue to be effective; •ensure that responsibility for monitoring compliance with the policies is independent of the persons implementing the policy, to allow the monitoring to be unbiased; and •report any results to senior management	Medium	25 Jul	*Schedule in 12 month review of staff understanding of policies and procedures by way of questionnaire (annual training audit) * Create a log of incidents (failures against policy and procedures e.g. where a complaint has been received) and action taken, use log as evidence of compliance monitoring and remedial action taken * Internal audit / external audit.	Training records Breach & near miss records		
14	Data protection awareness training has been provided for all staff.	You should brief all staff handling personal data on their data protection responsibilities. It is good practice to provide awareness training on or shortly after appointment with updates at regular intervals or when required. –Specialist training for staff with specific duties, such as, information security and database management and marketing, should also be considered.–The regular communication of key messages is equally important to help reinforce training and maintain awareness (for example intranet articles, circulars, team briefings and posters).	•provide induction training on or shortly after appointment; •update all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters); and •provide specialist training for staff with specific duties, such as marketing, information security and database management.	High	25-May	*Provide training to staff and stakeholders *Include DP awareness and training in induction processes	Training records Induction toolkit		Complete
15	There are written contracts with any data processors you use.	Whenever you use a processor you need to have a written contract in place.–The contract is important so that both parties understand their responsibilities and liabilities. The GDPR sets out what needs to be included in the contract.–In the future, standard contractual clauses may be provided by the European Commission or the ICO, and may form part of certification schemes. However at the moment no standard clauses have been drafted.–You are liable for your processor's compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor that adheres to an approved code of conduct or certification scheme may help you to satisfy this requirement – though again, no such schemes are currently available.–Processors must only act on your documented instructions. They will however have some direct responsibilities under the GDPR and may be subject to sanctions if they don't comply.———	•ensure that whenever your business uses a processor (a third party who processes personal data on your behalf) there is a written contract in place; •check both new and existing contracts now include certain specific terms, as a minimum, to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure). •determine whether it would be applicable to use standard contractual clauses from the EU Commission or a supervisory authority (such as the ICO) once drafted; •investigate whether there are any approved codes of conduct or certification schemes that may be used to help you demonstrate that you have chosen a suitable processor;	High	25 Jul	Create data processing contracts for processors where there are gaps.	Signed data processing agreements	Force procurement are preparing and issuing data processing amendments to existing contracts let on behalf of the OPCC Data processing contracts for HR and Payroll data dependent on data flow information from Force, this is awaited. Data processing agreement with Ideagen is being considered by Force procurement and IT services. A schedule of approved processing has been written by the OPCC and given to the Force.	Complete
16	information risks are managed in a structured way so that management understands the business impact of personal data related risks and manages them effectively.	You should set out how you (and any of your data processors) manage information risk.–You need to have a senior staff member with responsibility for managing information risks, coordinating procedures put in place to mitigate them and for logging and risk assessing information assets.–Where you have identified information risks, you should have appropriate action plans in place to mitigate any risks that are not tolerated or terminated.	•establish a clearly communicated set of security policies and procedures, which reflect business objectives and assign responsibilities to support good information risk management; •ensure there are processes in place to analyse and log any identified threats, vulnerabilities, and potential impacts which are associated with your business activities and information (risk register); and •apply controls to mitigate the identified risks within agreed appetites and regularly test these controls to ensure they remain effective	Medium	25 Sept	*review and update information security policy and procedures and share with staff. *Update information asset register, to identify information in more detail, assessed risk and mitigating actions *Create and Implement a data protection impact and risk assessment process to be completed for all new business activity / initiatives * Carry out a data protection impact and risk assessment for all existing personal data processes (where not already done)	Information security policy and procedures Information asset register Data protection impact assessment tool Process for testing controls		Complete
17	There are appropriate technical and organisational measures to integrate data protection into your processing activities	Under the GDPR, you have a general obligation to implement appropriate technical and organisational measures to show that you have considered and integrated data protection into your processing activities. Under the GDPR, this is referred to as data protection by design and by default.–You should adopt internal policies and implement measures which help your organisation comply with the data protection principles – this could include data minimisation, pseudonymisation and transparency measures———	•look to continually minimise the amount and type of data you collect, process and store, such as by undertaking regular information and internal process audits across appropriate areas of the business; •pseudonymise the personal data where appropriate to render the data record less identifying and therefore reduce concerns with data sharing and data retention; •regularly undertake reviews of your public-facing documents, policies and privacy notice(s) to ensure they meet the renewed transparency requirements under the GDPR; •ensure any current and/or new processes or systems enable you to comply with an individual's rights under the GDPR; and •create, review and improve your data security features and controls on an ongoing basis.	Medium	25 Sept	*Update data protection policy, to include requirements *write data protection procedures ie to specify when and how information audits will be undertaken *Carry out data protection impact assessment for all new initiatives to identify what the minimum data requirements are *Schedule and carry out an annual review of personal data held, and where held, and weed in accordance with information rentention policy - pseudonymise, minimise where possible (to meet business need) *Schedule and carry out an annual review of public facing documents	Data Protection policy Data protection procedure Data protection information audit plan / schedule		Complete.

18	You know when you must conduct a DPIA and have processes in place to action this.	DPIAs help you to identify the most effective way to comply with your data protection obligations and meet individuals' expectations of privacy.–An effective DPIA will allow you to identify and fix problems at an early stage, reducing the associated costs and damage to your reputation which might otherwise occur.–You must carry out a DPIA when:–* using new technologies; and–* when the processing is likely to result in a high risk to the rights and freedoms of individuals.–Processing that is likely to result in a high risk includes but is not limited to:–* systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals;–* large scale processing of special categories of data or personal data relation to criminal convictions or offences; and–* large scale systematic monitoring of public areas.–The DPIA should contain the following information:–* a description of the processing operations and the purposes including, where applicable, the legitimate interests pursued by your business;–* an assessment of the necessity and proportionality of the processing in relation to the purpose;–* an assessment of the risks to individuals; and–* controls that you put in place to address any risks you've identified (including security).––	•establish a policy which sets out when you should conduct a DPIA, who will authorise it and how it will be incorporated into the overall project plan. A DPIA screening process may be a useful tool in determining whether a DPIA is required; •assign responsibility for completing DPIAs to a member of staff who has sufficient control over the project to effect change eg Project Lead/Manager; •where a DPIA is required, ensure the process is completed before the project begins; •ensure your process for completing a DPIA includes consultation with the DPO/ data protection lead, data processors, third party contractors and with the public/their representatives in most cases; •ensure the information contained within the DPIA complies with the requirements under the GDPR and that the results are detailed within a report; •where a DPIA indicates that the processing would result in a high risk and you are unable to mitigate those risks by reasonable means, ensure your business is aware to follow the ICO consultation process to seek its opinion as to whether the processing operation complies with the GDPR.	Medium	25 Sept	*Write a DPIA policy, process and create / adopt a DPIA tool	DPIA policy DPIA process DPIA toolkit		Complete
19	there is a DPIA framework which links to your existing risk management and project management processes	A DPIA can address multiple processing operations that are similar in terms of the risks, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing.–You should start to assess the situations where it will be necessary to conduct one: –* Who will do it?–* Who else needs to be involved?–* Will the process be run centrally or locally?–If the processing is wholly or partly performed by a data processor, then that processor must assist you in carrying out the DPIA. It may also be appropriate to seek the views of data subjects in certain circumstances––	•review your existing risk and project management processes and ensure there is consistency and links with your DPIA processes in place; •drive awareness of DPIAs across your business, and particularly amongst risk and project teams so that they understand the requirements; and •ensure DPIA documentation is readily available for staff to use and that staff have had training on how to conduct the assessment.	Medium	25-Sep	*Add to DPIA policy, process and tools. *Add to OPCC risk register (risk of DP non-compliance resulting in financial or reputational penalty, infringement of an individual's rights and freedoms.) *provide awareness raising session for OPCC staff to include DPIA policy, process and toolkit.	OPCC risk Register DPIA policy, process and toolkit DPIAs (completed DPIAs) Training records		Complete
20	There is a nominated a data protection lead or Data Protection Officer	It is important to make sure that someone in your business, or an external data protection advisor, takes responsibility for data protection compliance.–You may need to appoint a DPO. Any business can appoint a DPO but you must do so if you:–* are a public authority (expect for courts acting in the judicial capacity);–* carry out large scale systematic monitoring of individuals (eg online behaviour tracking); or–* carry out large scale processing of special categories of data or data relating to criminal convictions and offences.–The DPO should work independently, report to the highest management level and have adequate resources to enable your organisation meet its GDPR obligations. –The DPO's minimum tasks are to: –* inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.–* monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. –* be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).––	•designate responsibility for data protection compliance to a suitable individual; •support the appointed individual through provision of appropriate training; •ensure there are appropriate reporting mechanisms in place between the individual responsible for data protection compliance and senior management; •register the details of your DPO with the ICO; and •document the internal analysis carried out to determine whether or not a DPO is to be appointed, unless it is obvious that your organisation is not required to designate a DPO.	High	25-May	Identify DPO			BS & CS Manager to undertake role and where conflict of interest identified, alternative DPO to be nominated.
21	Decision makers and key people in your business demonstrate support for data protection legislation and promote a positive culture of data protection compliance across the business.	You should make sure that decision makers and key people in your business are aware of the requirements under the GDPR. –Decision makers and key people should lead by example, demonstrating accountability for compliance with the GDPR and promoting a positive culture, within your business, for data protection. –They should take the lead when assessing any impacts to your business and encourage a privacy by design approach. –They should help to drive awareness amongst all staff regarding the importance of exercising good data protection practices.––	•clearly set out your business's approach to data protection and assign management responsibilities; •ensure you have a policy framework and information governance strategy in place to support a positive data protection and security culture which has been endorsed by management; •assess and identify areas that could cause data protection or security compliance problems and record these on your business's risk register; •deliver training which encourages personal responsibility and good security behaviours; and •run regular general awareness campaigns across your business to educate staff on their data protection and security responsibilities and promote data protection and security awareness and compliance.	High	May - Sept	*regularly raise at Managers' meetings *include in CEOs newsletters *Detail responsibilities in DPP and P. *look into incorporating information governance into the governance framework *review induction and ongoing training plans / PDPs and include appropriate training (part of the planned HR development and wellbeing strategy).	Meeting agendas Newsletters Governance framework Induction plan HR strategy and delivery plan	Not all of the products are likely to be completed until later in the year due to other work pressures.	
Data security, international transfers and breaches										
22	Therre is an information security policy supported by appropriate security measures	You should process personal data in a manner that ensures appropriate security. –Before you can decide what level of security is right for you, you will need to assess the risks to the personal data you hold and choose security measures that are appropriate to your needs.–Keeping your IT systems safe and secure can be a complex task and does require time, resource and (potentially) specialist expertise. –If you are processing personal data within your IT system(s) you need to recognise the risks involved and take appropriate technical measures to secure the data. –The measures you put in place should fit your business's needs. They don't necessarily have to be expensive or onerous. They may even be free or already available within the IT systems you currently have.–A good starting point is to establish and implement a robust Information Security policy which details your approach to information security, the technical and organisational measures that you will be implementing and the roles and responsibilities staff have in relation to keeping information secure––	•develop, implement and communicate an information security policy; •ensure the policy covers key information security topics such as network security, physical security, access controls, secure configuration, patch management, email and internet use, data storage and maintenance and security breach / incident management; •implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with your security policy •implement periodic checks for compliance with policy, to give assurances that security controls are operational and effective; and •deliver regular staff training on all areas within the information security policy.	High	25-Jun	*Review and update information security policy *Write information security procedures. *Include a 6 month review of information security compliance in DP procedure *Review training delivered, and arrange training as required *Add periodic information security training to training schedule	Info security policy Info security procedures DP procedure and DP information audit plan / schedule.		Complete
23	There is an adequate level of protection for any personal data processed by others on your behalf that is transferred outside the European Economic Area	The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.–These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.–Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR––	•ensure that any data you transfer outside the EU is handled in compliance with the conditions for transfer set out in Chapter V of the GDPR; •ensure that there is adequate safeguards and data security in place, that is documented in a written contract using standard data protection contract clauses; and •implement measures to audit any documented security arrangements on a periodic basis.	Low		Data is not currently transferred out of the EU. Activity to be determined should this change. This will be identified as a need through a DPIA which will be undertaken for any new project /iniative that involves personal data. *Record in DPIA policy, procedure and toolkit (need to consider and plan for processing that results in data transferred outside of the EEA.	DPIA policy DPIA process DPIA toolkit		Complete
24	There is an effective processes to identify, report, manage and resolve any personal data breaches.	The GDPR introduces a duty on all organisations to report certain types of personal data breaches to the ICO and, in some cases, to the individuals affected.–A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. –You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals. –Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly and without undue delay.–In all cases you must maintain records of personal data breaches, whether or not they were notifiable to the ICO.–A notifiable breach has to be reported to the ICO within 72 hours of the business becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide additional information in phases. You should make sure that your staff understand what constitutes a personal data breach, and that this is more than a loss of personal data. –You should ensure that you have an internal breach reporting procedure in place. This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.–In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place––	•train staff how to recognise and report breaches; •have a process to report breaches to the appropriate individuals as soon as staff become aware of them, and to investigate and implement recovery plans; •put mechanisms in place to assess the likely risk to individuals and then, if necessary, notify individuals affected and report the breach to the ICO; and •monitor the type, volume and cost of incidents to identify trends and help prevent recurrences.	high	25 May	*Get a decision on whether the OPCC or Force will process data breach incidents for the OPCC *write or adopt a data breach policy and / or procedure and identify the appropriate individuals to receive the report. *if reporting is within OPCC, provide training for nominated individuals to enable them to investigate and implement recovery plans, assess risk and decide on reporting *Regardless of which organisation progresses a data breach, create a data breach log to record *Identify training for staff (compulsory) at a staff meeting	Personal Data Breach policy Personal Data Breach process Data breach log Analyises of logs in data breach log Training records	Currently we report data breaches to the CEO under the DP policy, and the CEO has in the past referred to the Force Information Assurance Department as we rely on Force DPOs as subject matter experts in this field. It is the Force DPO that evaluates, investigates and makes decisions about breach investigations and subsequent reporting to the ICO or appropriate body. This historical situation is likely because the data we process is generally police related data, and Data Protection practitioner expertise has not been present in the OPCC / police authority. Recommend that the OPCC has its own process.	Complete
25	There are appropriate security measures in place to protect data in transit, received by your organisation and transferred to another organisation	The DPA requires organisations to have appropriate technical and organisational measures in place to protect shared personal data. In some instances you may transfer personal data to another organisation but still remain responsible for its security. It is therefore important that you set out, and ensure compliance with, agreed levels of security in relation to the personal data being shared. Please see our information security checklist for hints and tips on how to improve the security of personal data held by your organisation. In addition, when transferring data between organisations appropriate measures should be taken to ensure the security of that data while in transit. This may include the use of encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files. Equally there should be equivalent security around paper documents in transit. Such controls might include the use of a reliable courier, other secure postage, use of locked containers or tamper evident packaging	The Data Protection Act (DPA) requires organisations to have appropriate technical and organisational measures in place to protect shared personal data. In some instances you may transfer personal data to another organisation but still remain responsible for its security. You should: •always use an appropriate form of transport eg secure courier for sensitive paper based personal data and encryption on email, secure file transfer protocol (SFTP) or Virtual Private Network (VPN) for electronic files; •minimise data being transported; •log the transfer in and out where appropriate and check to ensure that data is received; and •employ security measures to safeguard the data in transit such as tamper evident packaging, and storage on encrypted devices	high	25 May	*Update data protection policy to include this commitment (including the need to minimise the need to transport data). *write a process that includes how personal data will be transferred between organisations securely, (Force network, CJSM, EGRESS Switch, recorded delivery, personal delivery / collection, internal mail and collection from a police station etc.) and how documents should be safeguarded in transit (tyvek envelopes / double wrapped / return address / encrypted memory sticks etc), and how items will be logged out and in (Pentana Feedback).	Data protection policy Data transfer process		Complete
Management and organisational data sharing										
26	The organisation informs individuals about the sharing of their personal data.	The first principle of the DPA requires that you process personal data fairly and lawfully. In order for the sharing of personal data to be considered fair you need to explain to individuals how you will use their personal data and who you will share it with. it is good practice to include privacy policies on your website and any forms that you use to collect data. These shoudl clearly explain the reasons for using the data including any disclosures or sharing. the second principle of the DPA requires that you do not process personal data in any manner that is incompatible with your specified purposes. this means that if you want to use or share data for a reaons that was not covered in your privacy notice, you should consider obtaining prior consent to ensure the new use is fair.	In order for the sharing of personal data to be considered fair and lawful the Data Protection Act 1998 imposes a requirement on organisations to explain to individuals how they will use personal data which they collect and who they will share it with. In such data sharing contexts it is important to explain: •who you are; •why you are going to share personal data; and •who you are going to share it with – this could be actual named organisations or types of organisation; and •provide further information if the situation where the nature of the sharing is such that some aspects of it would not be in the "reasonable expectations" of the individual that you would use their data in that way in order to allow the sharing to be considered fair.	high	25 May	*include in privacy notices *Include in consent forms *write data sharing agreements for regular information sharing activity	Privacy notices Consent forms Data sharing agreements (most likely between OPCC and Force)		Complete.

27	There are communicated policies, procedures and guidance to all staff which clearly set out when it is appropriate to share or disclose data.	Your policies, procedures and guidance should set out how staff ought to respond to sharing requests in the appropriate manner. Data sharing must be done in a way that complies with the law, is fair, transparent and in line with the rights and expectations of the people whose data is being shared. Your policy should explain how compliance with these requirements will be achieved eg monitoring of information sharing logs, quality assessment of samples of instances of sharing. This policy should be communicated to all relevant staff eg via intranet.	Your policies, procedures and guidance should set out how staff ought to respond to sharing requests in the appropriate manner. You should: •have an appropriate policy in place setting out when it is appropriate to share and/or disclose data; •ensure your policy and processes have considered how staff will ensure that sharing is legal, how the accuracy of the data will be maintained and what security measures should be put in place prior to any sharing of information; •detail in your policy how compliance with these requirements will be achieved; and •communicate the policy framework to all staff	Medium	July		Suite of DP policies and procedures as detailed throughout this document Record of sharing with staff	See line 2		Complete
28	Responsibility has been assigned to an appropriate member of staff for ensuring effective data sharing	It is good practice to nominate a senior, experienced person to take on overall responsibility for information sharing, ensuring compliance with the law, and providing advice to staff making decisions about sharing. Your policy should make it clear who this person is and how they can be contacted. The nominated individual should also receive appropriate specialist training to allow them to fulfil this role	•appoint a suitable senior experienced person(s) and ensure the role is detailed within policy; and •provide suitable training to the individual(s) to enable them to fulfill the role	Medium	July	Assign data sharing responsibility to a member of staff (DP Officer)	Data protection and data sharing policy statement			Complete
29	Adequate training is provided on an ongoing basis for staff that are regularly required to make decisions regarding whether or not personal data should be shared with third parties	It is essential to provide appropriate training to staff that are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process. Such training can be incorporated into any training you already give on data protection, security, or legal obligations of staff. Once delivered effort should be made to maintain that awareness. Materials such as posters, office wide emails, intranet updates or data sharing content in newsletters could be employed to achieve this	Where measures have only been partially implemented, please select the appropriate actions from the detail below: It is essential to provide appropriate training to staff that are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role within the sharing process. You should: •provide adequate training on an ongoing basis for staff that are regularly required to make decisions regarding whether or not personal data should be shared with third parties; •ensure staff with specific responsibility for management or oversight of information sharing processes complete appropriate training to allow then to fulfil this role; and •maintain staff awareness through materials such as posters, office wide emails, intranet updates or data sharing content in newsletters	Medium	July	*GDPR training delivered to all staff - record completion. *Check Data protection training in induction is suitable and up to date *add appropriate refresher training to training schedules. *Locate and put up posters in the office	Training records Posters			Complete
30	You maintain a log of all decisions to share personal data and this is reviewed regularly.	Your business should be able to justify the reasons why you decided to share specific personal data. Such sharing should be lawful and comply with any statutory restrictions in place on your organisation. When a decision has been made regarding whether to share information or not you should record your decision and your reasoning (regardless of if you shared information) along with what information was shared and for what purpose, who it was shared with, when it was shared and if the information was shared with or without consent. You should review the log of sharing decisions on a regular basis to ensure that decisions to share data are well founded and compliant. You should also use the review to identify areas where large quantities of data are being shared routinely and whether there is a need to formalise this with an information sharing agreement, if one is not in place already.	Your business should be able to justify the reasons why you decided to share specific personal data. Such sharing should be lawful and comply with any statutory restrictions in place on your organisations. In addition there should be an appropriate legal basis under one of the gateways or "conditions for processing" set out in schedules 2 and 3 of the Data Protection Act unless a relevant exemption from the DPA applies. You should: •maintain a log of all decisions to share personal data. Review it regularly to ensure that decisions to share data are well founded and compliant. This also helps to identify areas where large quantities of data are being shared routinely and therefore there is a need to formalise this with an information sharing agreement; and •where you are sharing data routinely, implement appropriate data sharing agreements (DSA) with all parties which are reviewed on a regular basis and recorded on a central DSA Log	Medium	July	*review data sharing log	Data Sharing Register Data sharing process Schedule for review of data sharing register			Complete
31	There are agreed data sharing agreements with an appropriate legal basis with all parties with whom personal data is routinely shared or where large quantities of data are to be transferred. These agreements are regularly reviewed	In some instances you may need to agree and regularise the way you share personal data. This may become clear from the volume of ad hoc requests you receive from a particular organisation or due to the introduction of a new process which will require the sharing of large quantities of data. Prior to introducing a new information sharing agreement (ISA), you should complete and record a legal compliance assessment to ensure that your business has legal authority to share the information and that such sharing complies with the requirements of the DPA. Your information sharing agreement should address all risks relevant to the type of sharing you are undertaking, but at least, should address the following issues: * the purpose, or purposes, of the sharing; * the potential recipients or types of recipient and the circumstances in which they will have access; * the data to be shared (this should be kept to the minimum necessary for your purposes); * data quality – accuracy, relevance, usability etc; data security; * retention of shared data; individuals' rights – procedures for dealing with access requests, queries and complaints; * review of effectiveness/termination of the sharing agreement; and * sanctions for failure to comply with the agreement or breaches by individual staff. In order to ensure that information sharing arrangements still reflect the current needs of your business and are compliant with the DPA they should be reviewed regularly. Such reviews should address whether the data is still needed to fulfil the purposes for which it is being shared and whether the ISA reflect current data sharing arrangements.	In some instances you may need to agree and regularise the way you share personal data. This may become clear from the volume of ad hoc requests you receive from a particular organisation or due to the introduction of a new process which will require the sharing of large quantities of data. You should: •complete a legal compliance assessment prior to introducing a new information sharing agreement to ensure that your business has legal authority to share the information and that such sharing complies with the requirements of the Data Protection Act 1998; and •regularly review information sharing arrangements to ensure they still reflect the current needs of your business and are compliant with the DPA. Such reviews should address whether the data is still needed to fulfil the purposes for which it is being shared and whether the ISA reflect current data sharing arrangements	Medium	July	*Review data sharing agreements (most likely only with Force), but potentially with Audit.	Data sharing agreements			Complete
32	The Information Commissioner's Office (ICO) has been provided with a description of the individuals or organisations to whom you intend or may wish to disclose personal data.	If you process personal data you may need to record the types of data you hold and why on the public register of data controllers. This is called 'registration'. This registration should include details of other organisations or groups of organisations you intend to share personal data with. Your business should ensure that these details are kept up to date	Most organisations are required by statute to provide the ICO with certain details regarding their processing of personal information. When you intend to share personal data with another organisation or group of organisations you should: •check whether you need to update your ICO registration to describe this. When any part of the registration entry becomes inaccurate or incomplete, for example because you are now disclosing information to a new type of organisation, you must inform the ICO as soon as practical and in any event within 28 days. It is a criminal offence not to do this	High	May	Check ICO registration	ICO registration			PCCs not required to register with the ICO.