This template is adapted from that provided by the ICO. It should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

If you are leading a project to introduce or make changes to any major project involving the use of personal data, a Data Privacy Impact Assessment may be required (or if you are making a significant change to an existing process). The responsibility for the DPIA lies with the project lead although you should take advice from the Data Protection Officer. Ideally the DPIA should be ongoing from the beginning of the project, and the final outcomes should be integrated back into your project plan.

Once completed, the DPIA should be checked by the Data Protection Officer, and at that stage further recommendations may be added.

Submitting controller details

Name of controller	West Midlands PCC
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	Andrea Gabbitas (DPO) and XXXXX (Project lead)

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Replacing the West Midlands PCC website. Website will carry news and other information that is in the public domain, but will also contain personal information about elected officials, contractors and staff. There will also be a private section which will offer the opportunity for external parties to share information with us. We agreed that a DPIA is required as the website is one of the main ways in which PCC/OPCC communicates and holds data, and is undergoing a fundamental review.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?
The website is a vehicle for a variety of processing - see details in the specification below which includes details of all the processing.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

As described in specification

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

As described in specification

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

As described in specification

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals’ views – or justify why it’s not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Meetings with Comms Manager (project lead) and DPO to discuss this took place on 1 April 2019. We highlighted some actions (see spec below) which require the views of other people. There have been a series of meetings with the Head of Comms and the Chief Executive in the build up to the procurement exercise and the content of the specification was agreed as part of these discussions. We agree that this is sufficient, and further consultation with stakeholders is not required.

In order to address the issues identified by our review of the specification, various elements of information were required from the contractor, Formation Media, and the responses are in the Annex.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

In the majority of processing activity the lawful basis is the public task of the PCC. In some cases we use consent, and for this small number of cases details are provided in the specification table below.

In terms of compliance and proportionality:

- the privacy notice will be provided to anyone submitting information to the website.
- GDPR training is provided for all staff who assist with management of the website and more generally in the OPCC, and this covers all the DP principles including proportionality, and also compliance. Tom Turrell is project manager for the website, and he, together with Head of Comms will be the ‘owner’/gatekeepers for the website. We discussed proportionality, and data quality and the other questions highlighted in this step.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
We examined risk for each element of the spec, see table below.	Remote, possible or probable As described in specification	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5 – all included in spec – see below				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted As described in specification	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	XXXXX	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	n/a	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Andrea Gabbitas/Polly Reed	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice: During the meeting on 1 April we identified a number of potential risks and agreed some actions to undertake or ask other staff to assist with. The actions are identified in the specification, and these have been integrated into the project. Recommended: the security and technology safeguards to be reviewed after 12 months to ensure they are still fit for purpose.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	n/a	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	XXXXX	The DPO should also review ongoing compliance with DPIA

PCC WEBSITE SPECIFICATION ANALYSIS

	Data Protection query/Risk?	Agreed action
The DESIGN		
Branding: Incorporate PCC branding.	**Remote/minimal = low**	
Content: Picture and video led + ability for people to be able to click on video/picture and enlarge it.	Who will be in the pictures? Any consent needed? RISK- POSSIBLE	Risk can be adequately mitigated by: 1. Consent is obtained when pictures are taken (and mostly taken in public spaces, so no additional consent is required) 2. Designated administrators responsible for each area must 'police' the content, including pictures to ensure all are appropriate with DP rules.
Overall: Design must be slick, modern and simple. We want it to not feel like a public sector website.	**Remote/minimal = low**	
The FUNCTIONALITY		
Simple site: Create an effective, consistent and easy to use site.	**Remote/minimal = low**	
Easy publishing: Real-time, easy to use content management facilities. Minimal training input with drag and drop functionality etc.	**Remote/minimal = low**	
Intelligent search: An intelligent search engine makes finding information quick and easy, learning from user behaviour. Power in the hands of the user through strong filtering tools.	Learning from user behaviour? Does this involve monitoring individuals? If so, what is the legal basis?	To be developed further in the next website update. Cookie policy in on website, and no further monitoring currently takes place

Newsletter: We need a simple form so people can sign up to the newsletter.	What will be the legal basis for this? Where will the privacy notice sit? **Possible/Minimal = low**	This will be consent based, for newsletter and news alerts. Copy of privacy notice will be provided and there will an 'unsubscribe' function. **Tom** to pass to FM for action.
Social Media: We need the ability to bounce users from the website straight to our social media platforms.	Does this require their consent? Will any personal data be gathered? **Remote/minimal = low**	No data gathered, as they will need to click to be re-directed.- - which acts as consent to go straight to the link.
Jobs: New online work experience application form to be embedded. We also need people to be able to sign up to job alerts.	Need to include confirmation that they have read and understood our privacy notice. Does current privacy notice need updating to include this? **Remote/minimal = low**	Need to introduce an 'accept' button that they have read the privacy notice, before they can continue. Not currently actioned, but this will be kept under review
Mobile first: Content templates should be fully flexible across desktop, tablet and mobile. Allowing access any time on any device.	**Remote/minimal = low**	
Form Creation: Be able to create forms with the ability to attach files on upload.	**Remote/minimal = low**	

Partially sighted: Keep current functionality for partially sighted people.	**Remote/minimal = low**	
Knife bin map: showing where all the knife bins are in the West Mids. We need to be able to add to this map as new bins are installed.	**Remote/minimal = low**	
Stop and Search map: This already exists, but just needs embedding	Would it be possible to identify individuals from the map?	Checked, and no it is not possible
Calendar: For meeting which contains agenda papers etc (see West Mids Combined authority one for guidance)	**Remote/minimal = low**	
Slideshow: revolving pictures on front page and ACF page	Do pictures include identifiable people?	Response – will only use pictures that are already in the public domain, or will use consent.
The Joint Audit Committee: needs its own webpage with a separate colour scheme so users can see it is not controlled by the PCC, but is just hosted on PCC website.	**Remote/minimal = low**	
News articles 1: We need them to automatically generate a publish date.	**Remote/minimal = low**	
News articles 2: We need to be able to auto-schedule news articles.	**Remote/minimal = low**	
News articles 3: Users need to be able to sign up to news alerts. We use Mailchimp so it would have to	Would any personal data be gathered on our website, or is it just automatic direction	Same as above.

<table>
<tr><td>seemless access and talk to that system without us having to do anything.</td><td>to Mailchimp? If yes, need to ensure a link to privacy notice, and gain consent.
<b>Remote/minimal = low</b></td><td colspan="2"></td></tr>
<tr><td><b>URLs:</b> We need to be able to continue to edit our URLs.</td><td><b>Remote/minimal = low</b></td><td colspan="2"></td></tr>
<tr><td><b>Auto-expire:</b> We need the ability to auto-expire pages. So when we publish a public consultation it will auto remove from the website when the consultation finishes.</td><td><b>Remote/minimal = low</b></td><td colspan="2"></td></tr>
<tr><td><b>Webcasting:</b> Audit page and Strategic Policing and Crime Board page needs the webcasting video embedded. See here: https://westmidspcc.public-i.tv/core/portal/webcasts</td><td>Is there possible inclusion of data in webcast
RISK – POSSIBLE
<b>Possible/minimal = low</b></td><td colspan="2">Agreed that it is sufficient to use the same processes as the beginning of SPCB meetings – warn people at beginning of event that it is webcast, and give them an opportunity to move/leave if they do not wish to be filmed.</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td>The SECURITY</td><td></td><td colspan="2">AG consulted Formation Media on the issues in this section in April 2019. The responses are in Annex A.</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">The Site (including Domain Name) must be protected against casual attack e.g. DDoS, Domain Spoofing, Web Host brute force and saturation.</td><td rowspan="4">These are the requirements in the contract,</td></tr>
<tr><td colspan="3">Costs/options for higher level of attack would be useful to know costs of e.g. sustained/organised attack, targeted attack e.g. state actors, and Insider Threat protection.</td></tr>
<tr><td colspan="3">The encryption in use for all components must meet minimum standards:</td></tr>
<tr><td colspan="3">Use the TLS 1.2 suite by default. TLS 1.0, SSL2/3 must not be used.</td></tr>
</table>

Certificate length must be 2048bits or higher.		stipulated by the OPCC
Use SHA2 e.g. SHA256 for hashing, SHA1 must not be used.		
Negotiation cypher must match the key length where possible e.g. DH group 14 for 2048bit, and utilise Forward Secrecy for ephemeral key exchange for sessions.		
Where possible, Diffie-Helmann Elliptic Curve keys should be used (ECDHE) as these are currently considered the most secure by the NCSC. Where ECDHE are not supported (some hardware still does not support this e.g. the Forcepoint firewalls), then appropriate RSA keys should be used for encryption at a minimum of 128bit, preferably 256bit.		
Ensure that server/clients disable weaker cipher and hashing suites e.g. MD5, RC4, SHA1 so that they cannot negotiate outside of the accepted cipher parameters above.		
Supplier must demonstrate appropriate security controls for physical and logical access to their datacentre hosting platforms. This includes personnel security management, physical datacentre protection, logical access to equipment and services, and any delegated permissions and access for support staff e.g. Follow The Sun support would imply that non-UK staff would have administrative access during out of hours support, which needs to be known.		
The site must be able to utilise functions to remove weaknesses in onward notifications e.g. an e-mail submission through the site should be an integrated web form or similar secure module, as opposed to any links and exposure of direct mail addresses.		
Back-end communication via e-mail services should utilise SMTPS (Secure) and be compatible with DKIM, SPF and DMARC for domain authenticity checks and mail assurance between any servers and mail services that the organisation uses (WMP utilise all three technologies and the PCC inherits this by using a WMP-provided e-mail address).		
The TECHNOLOGY		
Strong analytics component – A strong analytics and data gathering component is crucial to identify new opportunities, resolve issues and understand user behaviour.	**Remote/minimal = low**	This is looking at trends, but will be anonymised to such an extent that personal data will not be gathered
Flexible User admin structure – Ability to create, edit and allocate users to functional roles (e.g. writer,	Who will manage and monitor these roles, and ensure that only staff with	All staff in the OPCC are DP trained, and Head of Comms will allocate the roles.

publisher etc.) and to limit their editing to certain authorised parts of the site.	DP training are allowed to do it? **Possible/minimal = low**	
Support for all media types and files – From pics to video we need to be able to easily upload all popular media files. We also need to be able to embed external sites like Youtube, Vimeo etc.	**Remote/minimal = low**	
Version History – Content that is created should have version history to see who edited the file and have the ability to rollback.	**Remote/minimal = low**	
Media Library – Have the ability to have assets docs, Images, pdf, excel files to a media library. So we have the ability to reuse assets.	Who and how will the document retention of items in the library be managed?	**Document retention schedule managed by Comms Team**
Calendar and Events - Have the functionality where users can create events and they are stored in an online calendar.	Could include details of people attending events, but only staff/SPCB members in their public role **Remote/minimal = low**	

Active Citizens Fund and Custody Visiting sections for the new website

These areas of the new website will be subject to the same technology and security requirements as indicated above and below in the Annex.

Annex A: security considerations – these considerations were discussed at the meeting on 1 April, and further information was obtained from Formation Media.

Security Questions	**Response/mitigations in place**	**RISKS**
The Site (including Domain Name) must be protected against casual attack e.g. DDoS, Domain Spoofing, Web Host brute force and saturation.	The server protect against attacks in a variety of ways, including: • Automatic blocking of IPs after a set number of failed attempts. • DDoS is prevented via the server's core software.	Remote/significant =
Costs/options for higher level of attack would be useful to know costs of e.g. sustained/organised attack, targeted attack e.g. state actors, and Insider Threat protection.	Costs for these services can have a large range, which can include dedicated firewall hardware (in addition to software), additional web server software, website plugins, failover servers.	n/a
The encryption in use for all components must meet minimum standards:		**Remote/minimal = low**
Use the TLS 1.2 suite by default. TLS 1.0, SSL2/3 must not be used.	The server uses TLS v1.2	**Remote/minimal = low**
Certificate length must be 2048bits or higher.	The certificate length is 2048bits	**Remote/minimal = low**

Use SHA2 e.g. SHA256 for hashing, SHA1 must not be used.	The SSL certificates utilise SHA256 hashing	**Remote/minimal = low**
Negotiation cypher must match the key length where possible e.g. DH group 14 for 2048bit, and utilise Forward Secrecy for ephemeral key exchange for sessions.	Forward Secrecy is in use.	**Remote/minimal = low**
Where possible, Diffie-Helmann Elliptic Curve keys should be used (ECDHE) as these are currently considered the most secure by the NCSC. Where ECDHE are not supported (some hardware still does not support this e.g. the Forcepoint firewalls), then appropriate RSA keys should be used for encryption at a minimum of 128bit, preferably 256bit.	ECDHE keys are in use.	**Remote/minimal = low**
Ensure that server/clients disable weaker cipher and hashing suites e.g. MD5, RC4, SHA1 so that they cannot negotiate outside of the accepted cipher parameters above.	These ciphers are not is use.	**Remote/minimal = low**
Supplier must demonstrate appropriate security controls for physical and logical access to their datacentre hosting platforms. This includes personnel security management, physical datacentre protection, logical access to equipment and services, and any delegated permissions and access for support staff e.g. Follow The Sun support would imply that non-UK staff would have administrative access during out of hours support, which needs to be known.	Our hosting datacentre (where our main websites are stored) is on the premises of an old bank datacentre so it was purpose build to be secure. The compound is locked and gated and only those with a prior appointment are allowed on-site. All staff at the datacentre are DBS checked. Permission to servers are limited to approved support staff.	**Remote/significant = medium (in the case of a breach it would be high risk, but likelihood is deemed to be low)**

	To help deal with any fires, all staff on-site have access to server hardware in the event of a fire.	Appropriate mitigations are in place
The site must be able to utilise functions to remove weaknesses in onward notifications e.g. an e-mail submission through the site should be an integrated web form or similar secure module, as opposed to any links and exposure of direct mail addresses.	All forms are processed via the website to the relevant contact. No personal contact details are viewable outside of what has been requested. When submitting these forms, invisible captcha is utilised to prevent spam/robotic submissions in an easy to use manner that doesn't block or interrupt the user.	**Remote/minimal = low**
Back-end communication via e-mail services should utilise SMTPS (Secure) and be compatible with DKIM, SPF and DMARC for domain authenticity checks and mail assurance between any servers and mail services that the organisation uses (WMP utilise all three technologies and the PCC inherits this by using a WMP-provided e-mail address).	The website can be configured to use a specific email address and technologies to secure the connection. The main website utilises DKIM and SPF to improve security. In this case, these security measures are processed by WMP's email hosts, and we connect via SMTPS.	**Remote/minimal = low**
Intelligent search: An intelligent search engine makes finding information quick and easy, learning from user behaviour. Power in the hands of the user through strong filtering tools. Whether the search function on the new website will gather data on individuals and monitor them	The user will be able to filter pages by time published and category. Search results will be in order or relevance and feature a "did you mean?" suggestion to help the user find relevant information. When using the search, no personal data is stored.	**Remote/minimal = low**
Newsletter: We need a simple form so people can sign up to the newsletter.	A privacy notice is always good to have to offer additional assurance that their data isn't stored or used in a non-offending manner.	Privacy Notice updated bi-annually, and most recently 2021

Is a privacy notice needed in your opinion? If so, we will provide it and perhaps it could appear like a 'terms and conditions' form	Commonly these are linked to where relevant, so for the newsletter, the privacy notice will be linked within the newsletter section.	
New online work experience application form to be embedded. We also need people to be able to sign up to job alerts. Need to include confirmation that they have read and understood our privacy notice. Does current privacy notice need updating to include this?	This is another example of the privacy policy being linked to a single page so different pages/functionality can link to the privacy statement. Privacy policy will be reviewed to ensure this function is adequately covered.	Mitigations deemed adequate.
Media Library – Have the ability to have assets docs, Images, pdf, excel files to a media library. So we have the ability to reuse assets. Who and how will the document retention of items in the library be managed?	Default on the website platform. Retention rules and management are the responsibility of the client OPCC has a retention policy, and the Comms Team will manage the documents in accordance with this policy (a copy has been provided to all staff)	**Remote/minimal = low**