



Force Policy Framework (Surrey and Sussex) (700/2025)

Abstract

This document details how Surrey Police and Sussex Police will create and maintain policies. Also includes the review process and the implementation of new policies.

Policy

1. Introduction

1.1 This policy is required to ensure that Surrey Police and Sussex Police (hereafter referred to as the Forces) policies are written in a consistent format and are reviewed every 2 years.

2. Scope

2.1 This policy and its associated procedures provide instruction needed for the creation, review, maintenance and ratification of all Forces' policies. Instructions are provided to assist when changing a standalone Force policy to a joint Forces policy.

2.2 It also provides a process for ensuring that policies are not created when simple guidance would suffice and details the archiving process when a policy is no longer required, and how to request a copy of an archived policy.

3. Policy Statement

3.1 The Forces ensure policies both current and archived are available to officers and staff via the Force's policy sites found on the intranet. Policies are published externally in accordance with the Freedom of Information (FOI) Act 2000 unless publication / dissemination to individuals outside of the Forces could cause an operational risk to the organisation or their officers and staff.

Procedure

1. Policy, Authorised Professional Practice (APP) and the National Decision Model (NDM)

1.1 Force policies govern most of the tasks we undertake to carry out our roles. The policy is a short statement of the Forces intention.

The policy comprises of 3 sections.

1. Introduction. Why policy is needed, who it applies to.
2. Scope. What information is contained, which processes are covered.
3. Statement. What will be achieved by implementing the policy.

The procedure describes the major tasks required to achieve the objective / goal outlined in the policy. They contain mandatory instruction describing the processes which need to be followed. The procedure can contain links to guidance documents, templates or forms to assist colleagues.

1.2 The Forces hold policies in two categories.

1. Where they are required through Acts of Parliament e.g.

- UK General Data Protection Regulations (UKGDPR)
- Data Protection Act 2018
- Health and Safety at Work Act 1974
- Freedom of Information (FOI) Act 2000

2. Where they are required by the Forces to explain what we must and must not do to minimise risk.

1.3 APP: Where APP is available it will be followed by the Forces unless there is deviation. In this instance the Forces will write their own policies. Where APP is referred to it must be hyperlinked, sections of text must not be copied.

1.4 NDM: Where policies are not available through the respective Force's policy sites and guidance not available on the intranet officers and staff must use the NDM along with appropriate risk assessments e.g., Threat, Harm, Risk, Investigation, Vulnerability and Engagement (THRIVE).

2. Ownership

2.1 Policies are owned by the Forces Chief Constables with maintenance or implementation devolved to the risk owner of the area of business.

2.2 The Forces policies must have an owning department and a policy owner this will either be a Chief Superintendent / Superintendent or a police staff equivalent. The policy owner will typically assign a policy review to an expert on the subject, these are known as Single Point of Contacts (SPOCs) in Surrey and policy authors in Sussex. When a policy owner moves roles, it is their responsibility to contact the respective Force Policy Officer and provide the new owner's details. The Policy Officer's role is to ensure the Force's policies meet the standards described in this policy, they will provide individual support if required to ensure those standards are met. However, they are not subject experts and cannot write policies on the owner's behalf.

3. Review of an existing Surrey standalone policy

3.1 Mandatory 2-year review period

Force policies are subject to a 2-year mandatory review to ensure the information contained is current. Review dates are not extended. When a policy is overdue it is noted as such on the Policy Record Log and subsequently at Security and Information Management Board (SIMB) it is the responsibility of the policy owner to ensure their policies are reviewed on time.

3.2 The individual who reviews the policy must be an expert on the subject as the policy is subject to scrutiny and the individual writing the policy must be able to either answer questions regarding the topic or know how to find the information. Where an individual is asked to complete a review, and they are not confident with the topic they must raise this with the policy owner.

3.3 Reviews are sent to the area of business Single Point of Contact (SPoC), these are sent as a block according to how many there are to be reviewed. This is done once a month. The SPoC will send to the relevant subject owner.

Review documents are provided on a Word document as updates must never be made directly on the policy site. Only the documents provided must be used for the review and they include the policy, appendices (documents attached to the policy), the current Policy Workbook and a list of the previous policy stakeholders. Documents held elsewhere on the intranet and referred to within the policy will not be supplied and it is the policy authors responsibility to ensure the links are in working order and the information is correct.

All documents must be marked with the appropriate Government Security Classification (GSC). Handling instruction(s) must be added when marking Official or Official Sensitive) added / updated if applicable. Refer to section 9.

3.4 Before starting a review, it must be considered if the policy is still required. As processes develop and departments evolve the topic maybe covered by another Department's policy, intranet guidance or is available on APP. It is important to consider this point because if the same topic is available via other sources the audience will be unsure which process to follow. Refer to Archiving Policies at section 8.

3.5 Review steps

The author reviews the current policy, supporting documents attached to the policy, and hyperlinks to ensure the information is correct. If you decide that your current Surrey standalone policy should become joint, please follow the instructions at section 5.

When updating the policy / supporting documents use red font for new text and for text to be deleted strikethrough the text using the ~~ab~~ function. The tracked change function is not to be used. Ensure that gender neutral language is used throughout, use quotation marks or state as quoted when referencing legislation which is often gender specific. Be conscious of the use of Must and Should – “Must” is a mandatory instruction – “should” is guidance. Formatting / accessibility requirements at section 5.6 are to be followed.

The first appendix in the policy will be Appendix A: as appendices are added in sequence if the location changes during the review remember to update accordingly. Ensure document titles for the appendix are fairly short.

Ensure that gender neutral language is used throughout, use quotation marks or state as quoted when referencing legislation which is often gender specific. Be conscious of the use of Must and Should – “Must” is a mandatory instruction – “should” is guidance.

Complete / update the Policy Workbook. Refer to section 4.7 for details.

Email the reviewed policy, appendices and Policy Workbook to your stakeholders for their view, comments, or confirmation that the information is correct and is easy to understand. Email the documents showing the red font and strikethrough as they may want to compare the information. Refer to the stakeholder engagement at section 4.8 for details.

When you have completed the steps above submit all documents to a Policy Officer who will start the formal policy assurance consultation.

Surrey policies email Policy and Procedure.

It is important to note that a submission does not mean that your policy review is finished. The policy stays as a draft until the following has been completed.

- Formal policy assurance consultation
- You have responded to comments made during the consultation and returned documents
- Ratification has been requested and returned from policy owner

3.6 All documents must be marked with the appropriate Government Security Classification (GSC), a handling instruction must be added when marking Official or Official Sensitive) added / updated if applicable. Refer to section 9.

3.7 When you have completed the steps above submit all documents to Policy and Procedure to start the formal policy assurance consultation.

It is important to note that a submission does not mean that your policy review is finished. The policy stays as a draft until the following has been completed.

- Formal policy assurance consultation.
- You have responded to comments made during the consultation and returned documents.
- Approval has been requested and returned from policy owner - this will either be a Chief Superintendent, Superintendent or a police staff equivalent.
- Confirmation that the document can be published on the Surrey Police Website. Please refer to sections 9 and 10 for details.

4. Reviewing an existing joint Force / Sussex standalone policy

4.1 Mandatory 2-year review period

Force policies are subject to a 2-year mandatory review to ensure the information contained is current. Review dates are not extended. When a policy is overdue it is noted as such on the Organisational Reassurance Board (ORB) papers for compliance reasons. The Sussex Policy Officer will provide notification that the policy review date is approaching, but it is the responsibility of the policy owner to ensure their policies are reviewed on time.

4.2 The individual who reviews the policy must be an expert on the subject as the policy is subject to scrutiny and the individual writing the policy must be able to either answer questions regarding the topic or know how to find the information. Where an individual is asked to complete a review, and they are not confident with the topic they must raise this with the policy owner.

4.3 Review notification

A total of 3 emails are sent to the author advising them of the review date. The 1st email provides the review due date, instructions and the documents needed to complete the review, the 2nd is a reminder. The final email is to advise that the review date has passed, and the policy is overdue for its review.

4.4 Review documents are provided on a Word document as updates must never be made directly on the policy site. Only the documents provided must be used for the review and they include the policy, appendices (documents attached to the policy), the current Policy Workbook and a list of the previous policy stakeholders. Documents held elsewhere on the intranet and referred to within the policy will not be supplied and it is the policy authors responsibility to ensure the links are in working order and the information is correct.

All documents must be marked with the appropriate Government Security Classification (GSC). Handling instruction(s) must be added when marking Official or Official Sensitive. Refer to section 9.

4.5 Before starting a review, it must be considered if the policy is still required. As processes develop and departments evolve the topic may be covered by another department's policy, intranet guidance or is available on APP. It is important to consider this point because if the same topic is available via other sources the audience will be unsure which process to follow. Refer to Archiving Policies at section 8.

4.6 Review steps

The author reviews the current policy, appendices (documents attached to the policy) and hyperlinks to ensure the information is correct. If you decide that your current Sussex standalone policy should become joint, please follow the instructions at section 5.

When updating the policy / appendices use red font for new text and for text to be deleted strikethrough the text using the function. The tracked change function is not to be used.

Formatting / accessibility requirements at section 5.6 are to be followed.

The reader needs to know there is information and its relevance in an appendix therefore you need to refer to it in the main procedure (the procedure that sits under the policy). You can do this in a number of ways. A new section can be created or embed a reference to a section where it is relevant. The first appendix in the policy will be Appendix A: as appendices are added in sequence if the location changes during the review remember to update accordingly. Ensure document titles for the appendix include 'procedure' or 'guidance' (a procedure is mandatory instruction and guidance is optional). Try to keep the titles fairly short.

Ensure that gender neutral language is used throughout, use quotation marks or state as quoted when referencing legislation which is often gender specific. Be conscious of the use of Must and Should – “Must” is a mandatory instruction – “should” is guidance.

Complete / update the Policy Workbook. Refer to section 4.7 for details.

Email the reviewed policy, appendices and Policy Workbook to your stakeholders for their view, comments, or confirmation that the information is correct and is easy to understand. Email the documents showing the red font and strikethrough ~~ab~~ as they may want to compare the information. Refer to the stakeholder engagement at section 4.8 for details.

When you have completed the steps above submit all documents to a Policy Officer who will start the formal policy assurance consultation.

Joint policies email either Policy and Procedure (Surrey) or Policy Officer (Sussex).

Sussex standalone policy email Policy Officer (Sussex).

It is important to note that a submission does not mean that your policy review is finished. The policy stays as a draft until the following has been completed.

- Formal policy assurance consultation
- You have responded to comments made during the consultation and returned documents
- Ratification has been requested and returned from policy owner

4.7 Policy Workbook

You must ensure you complete the Policy Workbook. For assistance with sections 1 and 2 refer to the Equality Act 2010 and the Human Rights Act 1998. Also to assist there is the College of Policing training on Equality Impact Assessment (EIA) completion video and guidance documents EIA - ACAS Managers Guide, EIA - Toolkit Guidance and EIA - Designing for Accessibility these can be found on the intranet How do I? Equality and Diversity.

The Policy Workbook contains the following sections.

1. EIA Review
2. Human Rights Review
3. Code of Ethics
4. Implementation and Monitoring Plan
5. Freedom of Information Review – (external publication / dissemination)

4.8 Stakeholder Engagement

When either writing a new policy or reviewing an existing policy, the policy framework requires authors to engage with key stakeholders from relevant departments, staff networks / associations or external partners. Key stakeholders are those who have a vested interest or will be most keenly affected by the policy. Stakeholders may be

specialists who need to understand the policy in their roles or who can offer insightful feedback or may be users of the services that are affected by the policy.

Stakeholder engagement is a dialogue to inform decisions and will provide specialist input making a robust policy. Engagement can be conducted via emails, meetings or phone calls. Be clear as to why you are approaching the stakeholder, you may need specific information, confirmation or you may want a general opinion. In some cases, the intended stakeholder may advise they are not best placed to offer feedback or that there is a more appropriate subject matter expert. In these cases, the policy draft is not to be forwarded but instead returned to the requestor with the details of the suggested alternative stakeholder.

There will be occasions when you cannot accommodate a stakeholder's input, in these cases you should respond with your reasons.

Provide details of your stakeholders, their comments and your actions on the Stakeholder Engagement template.

4.9 Formal policy assurance

Once the draft policy, appendices, Policy Workbook and stakeholder details have been submitted, your Force Policy Officer will submit to their Policy Assurance team.

The assurance teams combine subject experts from across the Forces (including staff networks) and shall be available to work in partnership with policy owners and authors to support the production and/or review of their policies. The teams will review submitted policy and other documentation within a two-week timeframe and record their comments via the 'virtual' consultation forum within SharePoint.

Any queries or comments raised are fed back to the author by a Policy Officer. The author is required to respond to each comment and where required update the policy or other documentation. The author is to log their response on the sheet provided, these include situations when the policy was not updated but the comment has been considered.

4.10 Ratification

When the draft policy has progressed through the steps above it will be emailed to the owner for ratification this will either be a Chief Superintendent / Superintendent in the relevant department or a police staff equivalent.

5. Creating a new policy (joint and standalone)

5.1 There are actions to be considered prior to the submission of a new joint or standalone policy. This is to ensure there is no duplication of information held locally or nationally. Prior to starting a new policy, you must:

- Search the Forces policy sites for existing documents covering the topic of the new document.
- Search APP - If a topic is fully covered by APP then a Force policy is not required.
- Consider whether the use of the NDM would be more appropriate.

5.2 If after consideration you identify an existing policy which can be amended to incorporate your changes, contact your Force Policy Officer who will advise on next steps.

5.3 Consider who the audience is. If the information relates to just one team, it should be saved onto the Information Hub in Surrey or in Sussex placed in the Departmental shared folders. If the information has a wider audience than just one team but is guidance (useful information but does not have to be followed) then this is not a Force policy, consider adding to a How Do I? (HDI) site.

5.4 If you believe a new policy is still required, use the appropriate template (found in section 13). If you are unsure of how to write a policy, consider requesting a meeting with the respective Force Policy Officer and/or review the policy sites for policies on a similar subject as a guide.

5.5 Ensure the policy is inclusive of all protected characteristics as defined by the Equality Act 2010 and that gender neutral language is used throughout. Use quotation marks or state as quoted when referencing legislation which is often gender specific.

5.6 Formatting / accessibility requirements

- When attaching documents to the policy ensure the document title matches the title referred to within the policy (refer to 4.6 for instructions on adding appendices as procedures or guidance). In Surrey additional documents are embed as hyperlinks (ensuring document title is fairly short due to SharePoint limitations) and in Sussex they are attached to the policy database as an appendix.
- Keep language clear and simple. Where possible use words that are familiar in everyday use.
- Be conscious of the use of Must and Should – “Must” is a mandatory instruction – “should” is guidance.
- When using acronyms ensure the first use is in full. Where this is not possible provide an explanation of its use. Do not assume that colleagues know the acronyms meaning or what you are referring to.
- Do not use an ampersand (&) or shorten a word e.g., don’t. Words are to be written in full.
- Use short paragraphs.
- Use Arial font in size 12.
- Use bulleted lists where order is not sequential or numbered lists where it is.
- Only use tables for data and when no other option is available. In Sussex a database is used to store policies and formatting is extremely limited.
- Only use black font (do not use colour for instructions).
- Always align text to the left.
- Do not use the italic function or underline function. Use bold to emphasize meaning.

- Do not use “click here” when embedding hyperlinks. Either provide the full link or the destination title.
- Add a date to the footer.

5.7 Assign an Owning Department and a policy owner of Chief Superintendent / Superintendent or a police staff equivalent who will be accountable for the policy ensuring the information is kept current and mandatory reviews are completed on time.

5.8 For joint and Sussex only policies (not needed for Surrey standalone), please complete the stakeholder engagement and Policy Workbook (refer to sections 4.7 and 4.8).

5.9 Submit all the documents and owner details to your Force Policy Officer who will complete the steps as detailed at section 4.9 Formal Assurance.

6. Policy updates (joint and standalone)

6.1 If a policy requires an amendment, this is known as a policy update. A request for an update must be from either the Policy Owner or an expert within the owning department. Updating a policy does not change the 2-year review date.

6.2 There are numerous reasons as to why a policy would require an update. When a minor update to a policy is required, a policy review is not required. To complete an update:

- In Surrey download a copy of the policy from the policy site.
- In Sussex contact the Policy Officer to request a copy of the policy.

Once you have the Word document, update using red font for new text and strikethrough ~~ab~~ the text to be deleted. The tracked change function is not to be used.

A major change to a policy would involve a full review or as a minimum a consultation with the affected department must take place.

6.3 The update request is kept on file for auditing purposes and noted on the Policy Routine Order.

7. Storage and Retention

7.1 Policies are retained in line with the Surrey and Sussex Retention Schedule.

7.2 Copies of policies must not be stored independently. Policies are constantly updated and the only way to be sure you are reading the correct version is to view the policy on the appropriate database. Links to the Forces policy sites can be found in the footer of the Intranet.

8. Archiving Policies

8.1 If it is decided that a policy and the supporting documents held on the policy sites are no longer required, they can be archived. Archived policies are kept for purposes such as audits or conduct hearings.

Authorisation from the policy owner is required to archive a policy. The authorisation should be emailed to the respective Force Policy Officer who will complete the archiving process and forward on the request to the other Force's Policy Officer to do the same.

Archived policies can be requested in Surrey by emailing Policy and Procedure (Surrey) and in Sussex they can be viewed using the search function on the policy database or by contacting Policy Officer (Sussex).

9. Government Security Classification

9.1 All Policies are Government Security Classification (GSC) of 'OFFICIAL' by default. This means they can be shared with members of the public / third party organisations under the Freedom of Information Act 2000 (FOI). It is the policy author / owner's responsibility to review the contents and amend the GSC to 'OFFICIAL - SENSITIVE' as required. The use of the marking Official – Sensitive does not mean a policy is automatically exempt from FOI requests. Authors and owners who consider a policy should not be disclosed should consult the respective Force Information Access Team or Data Protection Officer during the review process.

Any policy that has a GSC of 'OFFICIAL - SENSITIVE' must have:

- 'OFFICIAL – SENSITIVE' in the header and footer. Refer to the Surrey Police and Sussex Police Information Security Policy (722).
- Contain handling instructions (examples below):
- The information in this policy is for the exclusive use of Surrey Police / Sussex Police / the Forces.
- The information in this policy must not be passed on to any third party without the express written permission of (enter Department).
- The information in this policy may not be used for legal disclosure purposes without the express written permission of (enter Department).
- Be aware that any improper disclosure, copying, distribution or use of the contents of this information is prohibited and criminal proceedings may follow.

10. Publication Scheme

10.1 It is a requirement under the Publication Scheme and FOI that policies (reference includes procedures) are published on the Force's websites to ensure transparency in our operations and can provide advice to members of the public.

If the policy author does not want a specific policy to be shared under the FOI scheme, they will need to review and mark sections to be redacted. The policy author must consider the GSC marking (along with handling instruction(s)). If redactions are required, the following process takes place:

Step 1: Once the policy has gone through the assurance process, the final version of the policy will be ratified and published on the Forces policy sites by the Force Policy Officer.

Step 2: The author will be contacted to review for external publication. The author must review the content to ensure it is safe for public dissemination under FOI.

Step 3: The author must highlight the relevant sections to be redacted and send this back to their respective Force Policy Officer. All redactions must be struck through (~~ab~~) and highlighted.

Step 4: Once received, the Force Policy Officer will redact as per the authors instructions and publish externally.

Where there is no response to the request for redactions, the policy will not be published externally, and policy FOI requests will be forwarded to the policy author / owner for a response copying in the respective Force FOI team. For further information on FOI requests received by the Forces please refer to

Surrey: Freedom of Information (FOI) Requests for Information Policy

Sussex: Freedom of Information Policy (821)

11. Communication

11.1 Details of the policies which have been reviewed, are new, or those updated are added to the Policy Routine Order (RO) published weekly. The RO will also include details of archived policies.

12. Reporting

12.1 Policy portfolios are reviewed at various accountability meetings (overdue / current). The individual reviewing the policy may be asked to provide progress updates. It should be noted that these requests are outside of the policy review process and should be responded directly and not passed to the Policy Officer for a response.

12.2 All

Overdue policies will be subject to an escalation process and will be reviewed at the SIMB which is held monthly. These are reviewed by the Senior Information Risk Officer (SIRO) to ensure Force compliance.

12.3 Sussex standalone and joint Force

Policy statuses are reviewed at the ORB held every 3 months. When a policy is shown as overdue a rationale is required. The Policy Officer will email both the policy owner and author to request that a rationale be provided. When no response / rationale has been provided the ORB policy is noted as such.

Team: Corporate Development Department.