Suffolk Police and Crime Commissioner

Making Suffolk a safer place to live, work, travel and invest

ORIGINATOR: CHIEF EXECUTIVE	**DECISION NUMBER: 30 - 2025**

REASON FOR SUBMISSION:	**FOR DECISION**

SUBMITTED TO:	**POLICE AND CRIME COMMISSIONER**

SUBJECT:	**UPDATED GENERAL DATA PROTECTION POLICY**

SUMMARY:

The first edition of the Police and Crime Commissioner's General Data Protection Regulation Statement of Policy was published on 25 May 2018 on the date the General Data Protection Regulation (GDPR) became part of English Law. The second edition was introduced to accommodate changes that have arisen since that time including the complaints review duties.

This is the third edition and reflects the introduction of the UK General Data Protection Regulation which was introduced on 1 January 2021 and replaced the General Data Protection Regulation which had been in force since 2018. It also includes an updated retention scheduled developed after an audit of data held by the Office of the Police and Crime Commissioner (OPCC).

RECOMMENDATION:
It is recommended that the Police and Crime Commissioner adopts this policy.

APPROVAL BY: PCC
The recommendation set out above is agreed.

Signature: **Date**: 20 October 2025

DETAIL OF THE SUBMISSION

1. KEY ISSUES FOR CONSIDERATION:

1.1 The Police and Crime Commissioner for Suffolk (the PCC) is a statutory role established by the Police Reform and Social Responsibility Act 2011. The role has been established as a corporation sole meaning that the PCC is a separate legal entity. Whilst the role, functions and powers of the PCC are set out in the 2011 Act, the Policing Protocol Order 2023 also helpfully summarises the requirements and responsibilities placed upon the PCC.

1.2 The PCC, in providing a service as a public authority on behalf of the public, processes personal information. In processing personal information, the PCC must comply with the provisions of the UK General Data Protection Regulation (UK GDPR) which was introduced on 1st January 2020 and other relevant data protection legislation.

1.3 This document sets out the PCC's general approach and policy to the processing of personal information for the purposes of carrying out his statutory role and responsibilities in compliance with the UK GDPR and other relevant data protection legislation.

2. FINANCIAL IMPLICATIONS:

2.1 The agreement does not have any specific financial implications.

3. OTHER IMPLICATIONS AND RISKS:

3.1 There are no other known implications and risks.

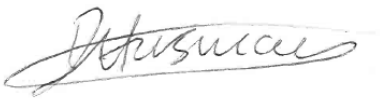
ORIGINATOR CHECKLIST (MUST BE COMPLETED)	PLEASE STATE 'YES' OR 'NO'
Has legal advice been sought on this submission?	**No**
Has the PCC's Chief Finance Officer been consulted?	**No**
Have equality, diversity and human rights implications been considered including equality analysis, as appropriate?	**Yes**
Have human resource implications been considered?	**Yes**
Is the recommendation consistent with the objectives in the Police and Crime Plan?	**Yes**
Has consultation been undertaken with people or agencies likely to be affected by the recommendation?	**No**
Has communications advice been sought on areas of likely media interest and how they might be managed?	**No**
Have all relevant ethical factors been taken into consideration in developing this submission?	**Yes**

In relation to the above, please ensure that all relevant issues have been highlighted in the 'other implications and risks' section of the submission.

APPROVAL TO SUBMIT TO THE DECISION-MAKER (this approval is required only for submissions to the PCC).

Chief Executive

I am satisfied that relevant advice has been taken into account in the preparation of the report and that this is an appropriate request to be submitted to the PCC.



Signature: **Date**: 26 September 2025

POLICE AND CRIME COMMISSIONER GENERAL DATA PROTECTION REGULATION STATEMENT OF POLICY

Chief Executive Third Edition 1 October 2025

Preamble

The first edition of this policy was published on 25 May 2018 on the date the General Data Protection Regulation (GDPR) became part of English Law. The second edition was introduced to accommodate changes that have arisen since that time including the new complaints review duties that now fall upon the Police and Crime Commissioner (PCC) as well as the Information Commissioner's report of August 2020 upon compliance by PCCs.

This third edition reflects the introduction of the UK General Data Protection Regulation which was introduced on 1 January 2021 and replaced the General Data Protection Regulation which had been in force since 2018.

The developments have, where appropriate, been addressed in a reasonable and proportionate way in this third edition of the GDPR policy.

Contents

First Edition – 25 May 2018

Second Edition – 1 November 2020

Third Edition – 1 October 2025

1. Introduction

The Police and Crime Commissioner for Suffolk (the PCC) is a statutory role established by the Police Reform and Social Responsibility Act 2011. The role has been established as a corporation sole meaning that the PCC is a separate legal entity. Whilst the role, functions and powers of the PCC are set out in the 2011 Act, the Policing Protocol Order 2023 also helpfully summarises the requirements and responsibilities placed upon the PCC.

The PCC, in providing a service as a public authority on behalf of the public, processes personal information. In processing personal information the PCC must comply with the provisions of the UK General Data Protection Regulation (UK GDPR) which was introduced on 1st January 2020 and other relevant data protection legislation.

This document sets out the PCC's general approach and policy to the processing of personal information for the purposes of carrying out his statutory role and responsibilities in compliance with the UK GDPR and other relevant data protection legislation.

The policy has been informed by an information audit conducted by the Office of the PCC with the explicit purpose of establishing the personal information that is held by the PCC, why the information is held, from where it came, where it is stored and with whom the information is shared.

The UK GDPR contains a number of statutorily defined terms. Foremost is the term personal data. Personal data is essentially any information that allows a natural person to be identified.

The UK GDPR also uses the term data controller. This includes a public authority which alone or jointly with others determines the purposes and means of the processing of personal data. The PCC is a data controller for the personal data he collects to discharge his statutory purposes. Numerous obligations and responsibilities attach to the role of data controller. Insofar as they impact upon the PCC they are set out in this policy.

The UK GDPR also uses the further term of data processor. This term includes a person, public authority or other body which processes personal data on behalf of the controller. Responsibilities and obligations attach to this role also.

The term "processing" means any operation or operations performed upon personal data, whether automated or not. This includes collection, structuring, storage, retrieval, use, disclosure, dissemination or erasure. The processing of data must comply with a number of rules which are largely captured within the data protection principles. These principles are:

Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that the PCC must tell the Data Subject what processing will occur (transparency); the processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the PCC must specify exactly what personal data is collected and for what it will be used.

Principle 3: Data Minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the PCC must not store any personal data beyond what is strictly required.

Principle 4: Accuracy

Personal data shall be accurate and kept up to date. This means the PCC must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. This means the PCC must, wherever possible, store personal data in a way that limits or prevents identification of the Data Subject.

Principle 6: Integrity & Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The PCC must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate, compliance with the Data Protection regulations in a practical and recorded way.

In summary, the PCC is a data controller for the purposes of the UK GDPR. The PCC both controls and processes personal data in the exercise of his statutory functions and the conduct of his business. This policy explains how he will do this.

2. Relationship with Suffolk Constabulary

The PCC, whilst a separate legal entity to the Chief Constable of the Suffolk Constabulary, has a close day-to-day working relationship with the Chief Constable. The Chief Constable is also a corporation sole. The relationship between the PCC and the Chief Constable is defined within the Police Reform and Social Responsibility Act 2011 and The Policing Protocol Order 2023.

The PCC and Chief Constable have agreed to work together in co-operation to ensure the effective and efficient delivery of policing services. The PCC's Scheme of Governance and Consent 2023 which is a foundation of the Governance Framework between the PCC and Chief Constable provides that, notwithstanding their separate legal identities as corporation sole, it is acknowledged that they have such interdependence as to require the sharing of significant areas of business support.

Accordingly, the sharing of business support, for example, Finance/Payroll, HR, ICT, Performance, Consultation, Legal, Vetting, is a co-operative arrangement for the effective delivery of business support essential to the operation of both corporation sole. By its very nature, the delivery of business support by the Chief Constable to the PCC means that personal data under the control of the PCC is processed by the Chief Constable. This is regulated by an agreement between the two corporation sole; between data controller and data processor.

In some circumstances the PCC will receive personal data from the Chief Constable where the Chief Constable is a data controller in order for the Chief Constable and PCC to discharge both their statutory obligations. This includes personal data where relevant to any aspect of the statutory arrangements between PCC and Chief Constable. One such example is in relation to Police Appeals Tribunals. This is regulated by the agreement between the PCC and Chief Constable. The complaints review responsibilities falling upon PCCs from 1 February 2020 involve the PCC receiving personal data from the Chief Constable to enable the PCC to discharge their statutory responsibilities. This too falls to be regulated by the agreement between the PCC and Chief Constable.

The relationship between the PCC and Chief Constable is such that, as appropriate, the policies of the Chief Constable are taken to apply within the Office of the Police and Crime Commissioner (OPCC).

3. The Data Collected and Held by the PCC

The PCC, as compared with other public authorities, collects a relatively small amount of personal data. The data they collect and hold is to enable the PCC to perform their statutory functions. The PCC and staff within the OPCC do not collect any data other than that used to discharge the statutory functions of the PCC and the OPCC. The personal data that is routinely collected and held can be categorised as follows and as relating to:

- Appointments to paid roles:
    - Chief Constable;
    - Audit Committee Members;
    - Legally Qualified Persons;
    - Independent Members of Misconduct Panels;
    - Employees of the PCC.
- Appointments to volunteer roles:
    - Custody Visitors.
- Contacts with whom the PCC liaises for the purposes of governance, dissemination of information, public and business meetings, surveys and consultations.
- Correspondents who write to the PCC.
- Complainants against the PCC, Chief Constable, or any of those appointments listed above.
- Applicants for any of the appointments listed above.
- Police Appeals Tribunals.
- Complaints Review.
- Miscellaneous personal data received from the Chief Constable in the discharge of the PCC's statutory responsibilities.

In relation to this personal data the PCC is a data controller. This is because he determines what data to collect and how it will be processed.

Information that is held concerning some of these categories comprises data that has been provided by the individuals themselves, or where ensuing inquiries have been made, the Chief Constable or referees (in the case of applications for roles).

Information relating to the paid appointments and volunteer roles is shared with the Chief Constable as described above. This includes for purposes relating, where appropriate, to finances and payroll, pension, HR, ICT and vetting. Information relating to correspondents and complainants may also be shared with the Chief Constable in order to enable the PCC to discharge his statutory roles. This includes dealing with complaints and providing the link between the police and communities. As indicated the data shared with the Chief Constable is regulated by an agreement. Information relating to complaints about the PCC may be shared with the Police and Crime Panel and their offices to enable the Police and Crime Panel to discharge its statutory role. This is done in compliance with the governing statutory regime.

Information relating to the Legally Qualified People and Independent Members of Misconduct Panels is common to the PCCs within the Region. The PCCs work together jointly to appoint and maintain Regional Panels of Legally Qualified People and Independent Members. To this extent the PCCs are all data controllers. This is regulated by agreement.

Appropriate personal data relating to Legally Qualified People, Independent Members of Misconduct Panels, Audit Committee Members, Employees, Custody Visitors is shared between each respective category where that is necessary to enable contact and interaction for the benefit of the particular business area. This is to be made clear as appropriate to all relevant categories of data subject.

Personal data relating to those areas described above are held variously by the PCC in hard copy, on site at the OPCC at Police Headquarters, Martlesham Heath or in storage, on the Information and Communications Technology computer drive system and in Outlook, the latter two of which are provided by the Chief Constable through the Suffolk Constabulary's ICT system. The ICT delivered by the Suffolk Constabulary is a secure system governed by the policies of the Suffolk Constabulary.

Where the PCC or his staff become aware that any personal data passed to a third party is inaccurate, that third party must be advised of the inaccuracy so that it can correct its own records.

4. Legal Foundation for Processing Personal Data

The data referred above as collected by the PCC is necessary for compliance with legal obligations to which he as controller is subject.

By legislation, associated guidance or codes of practice the PCC is required to appoint a Chief Constable, Audit Committee members, Legally Qualified People, Independent Members of Misconduct Panels and Custody Visitors. They are required to provide the link between the police and communities as well as working with partners and therefore can reasonably be expected to hold personal data in relation to the performance of these functions. They have responsibility for complaints against the Chief Constable; they may receive complaints about themselves; and their Chief Executive is responsible by delegation from the Police and Crime Panel for the initial receipt and handling of complaints about them as PCC. The PCC's staff and their statutory officers derive their authority to act on their behalf by their appointment by the PCC and through the operation of legislation and the PCCs Scheme of Governance and Consent.

The PCC employs staff to statutory and other roles within their office, acting through statutory powers vested in them as PCC. In this regard data processing is necessary for the entering into and purpose of the employment contracts.

The PCC discharges a number of statutory responsibilities and where they have a duty to act. This can involve the processing of personal data.

The processing of personal data as referred to above therefore satisfies the criteria for lawfulness of processing under the UK GDPR because its processing is necessary for compliance with a legal obligation to which the PCC as data controller is subject, and further, where appropriate, this position is fortified by either implied or actual consent. The legal support for collecting and processing the data is set out in Appendix A.

The PCC performs statutory functions and derives his authority from legislation. As such he has a legal foundation for processing personal data. The corollary of that is that neither the PCC nor OPCC should be involved in the processing of personal data either electronically or otherwise that is not connected or associated with the PCC or OPCC functions.

5. Privacy Notices

Transparency and providing accessible information to individuals about how their personal data will be used is a key element of the UK GDPR. The most common way to provide this information is in a privacy notice.

Accordingly, when data is collected from an individual they must be informed about what the PCC will do with their personal data. Individuals will require to be provided with a privacy notice which sets out all the privacy information that is made available to an individual when information is collected from them.

A privacy notice for the PCC should contain an explanation of:

- The identity and contact details of the PCC as data controller and collector of the data;
- The purposes and legal basis for processing the data (ie why is the data being collected);
- How the data will be used;
- Who the data will be shared with and why;
- How long the data will be retained;
- Individual rights under the UK GDPR.

A privacy notice will be required to be issued to data subjects. This includes those who apply for appointments (whether eventually appointed or not), contacts, correspondents and complainants, and as described above. In the case of applicants for appointments this requirement will arise at the point of application. In the case of others this will arise at the earliest available opportunity. In the case of those who apply for appointment, the PCC also infers implied consent to process personal data for the purposes of considering appointment, and if appointed, the subsequent discharge of the appointment duties and associated matters.

A generic privacy notice for those who apply for appointments can be found at Appendix B. This notice should be used for issue to all data subjects who apply for appointment (whether eventually appointed or not) at the point of application.

The personal data of some data subjects will of necessity be required to be shared with the Chief Constable and Suffolk Constabulary. This will be explained in the privacy notice.

6. Consent

In instances, for example, where a correspondent is raising issues about the PCC and/or the Constabulary, the form of privacy notice may need to be adapted for the purposes of obtaining consent in order to process their information. This section deals with situations where consent may be necessary or desirable.

Where consent is considered to be required from an individual in order to process their information the PCC will need to explain to the individual what is being asked of them and why. Consent is likely to be required where a correspondent is raising an issue with the PCC that requires information from or a response from the Constabulary. Alternatively, it may be required where information or a response is required from any other third party. The seeking of consent will go hand-in-hand with providing a privacy notice. Where there is the choice whether an individual's personal data is referred to the Constabulary or other third party it is important to make sure the individual has a choice and an opportunity to exercise it. Clearly refusal to give consent may prevent the PCC from giving or facilitating an appropriate response to a correspondent.

Accordingly in circumstances where it is necessary to pass personal data on to a third party to enable the PCC to respond to a correspondent or other individual in the performance of his statutory functions the PCC will seek consent using clear and plain language.

Whilst the consequences of not giving consent may be that the PCC cannot respond to a correspondent or individual as fully as may be possible the decision not to give consent needs to be made from a fully informed position. Consent will also be revocable and this needs to be explained in the form of consent.

The form of privacy notice providing for consent to be used for correspondents and complainants is found at Appendix C.

The form of privacy notice providing for consent to be used for contacts is found at Appendix D.

In the case of review of complaints dealt with by Suffolk Constabulary the PCC website advises that "by requesting a review, you are providing consent that you agree to the sharing of your personal data for the data for the purposes of progressing your review in accordance with the law and statutory guidance". Simply stated, without the implied consent the PCC is unable to conduct the review.

It must be remembered that the burden will be on the PCC as data controller to demonstrate, where consent is the legal basis for processing, that the consent was given. Accordingly, the data subject will, except as provided above, be required to advise their consent in writing.

7. Contracts and Commissioning

In the arrangements between the PCC and Chief Constable, set out in the Scheme of Governance and Consent, for the purposes of contracts and procurement, the PCC has overall responsibility for property and contracts. The PCC through the Scheme of Governance and Consent has granted consent to the Chief Constable for the daily administration of contracts in accordance with Financial Regulations and Contract Standing Orders. All contracts are required to be entered into in the name of the PCC.

The Chief Constable therefore has responsibility for the daily administration of contracts. The PCC requires the Chief Constable to ensure that all existing and future contracts are UK GDPR compliant. In this regard appropriate due diligence is undertaken by the Chief Constable's procurement function. Whereas the PCC is the data controller in relevant contracts, by virtue of his letting a contract or call-off from a Framework Agreement, the Chief Constable will also be a data controller/data processor. This will be provided for in the agreement between the PCC and Chief Constable.

In some instances the PCC himself may pass personal data under his control to a contractor. In that situation the PCC must ensure as data controller that where personal data is passed to a data processor, the contract ensures that the data processor complies with their UK GDPR responsibilities and obligations. The PCC has power to arrange for the provision of services that secure the reduction of crime and disorder or help victims, witnesses and others affected by offences and anti-social behaviour. It is unlikely that any UK GDPR issues arise for the PCC as data controller as the external organisations who are commissioned to provide such services are not using PCC data to meet the PCC's purpose. Notwithstanding this position, the services must be arranged under an agreement that places specific conditions on the external organisation that in relation to the service being commissioned the external organisation must ensure that any data processing carried out will meet the requirements of the UK GDPR and ensure the rights of the data subject. The standard form conditions for commissioning awards are appended at Appendix E.

Steps will need to be taken through contract monitoring arrangements to ensure that contract and commissioning conditions relating to UK GDPR are complied with.

8. Data Retention and Storage

Data retention is a form of data processing and as such is subject to all the requirements applicable to the specific purposes for which it was collected.

Data subjects must be informed of the retention of their data and their rights in relation to it.

The retention periods for data processed by the PCC are set out in Appendix F. For any personal data not covered by Appendix F, the retention periods in the policies of the Chief Constable will be applied. Data retained by the PCC will be regularly reviewed for consideration of accuracy, relevancy, UK GDPR compliance and deletion. Any inaccurate personal data shall be erased or rectified. For purposes of deletion personal data will not generally be retained beyond the time where the purpose for the data processing (including its retention) has ended. Retention should not be for longer than is necessary and consideration as to retention should be given against the time limits in Appendix F. If data is retained beyond the period specified in Appendix F the justification shall be recorded.

Data shall be stored in the ICT system whose use is provided to the OPCC by the Chief Constable, manual records or long-term storage (Deep Store) and where appropriate levels of security are afforded to the personal data, using appropriate technical or organisational measures, to ensure there is no unauthorised or unlawful processing and accidental loss, destruction or damage.

The PCC and staff shall take all reasonable steps to provide for the security of personal data including ensuring that workstations, both desk and screen, are kept free of personal data when not in use or unattended.

9. Individual Rights of the Data Subject

Right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR and is provided for through a variety of methods set out above including the use of a Privacy Notice.

Through this process we provide individuals with information including: the purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with.

Rights of Access

An individual who makes a written request is entitled to be told whether or not any of their personal data is being processed. If this is the case then the individual is entitled to be advised of the description of the personal data, the purposes for which it is being processed, recipients, retention periods and rights of rectification, erasure, restriction and objection. A data subject has a right to be given a copy of the information comprising the data and given details of the source of the data.

Where access is requested all reasonable measures to verify the identity of the data subject should be adopted before access is given.

The first copy of information provided in response to a subject access request must be provided free of charge. Thereafter a reasonable fee that reflects administrative costs may be charged.

Where the request is excessive or repetitive, either a fee can be charged in respect of administration costs or the request can be refused. In the case of the latter, the reasons must be provided to the data subject. Information about their right to make a complaint to the Information Commissioner's Office must also be provided with this communication.

Subject access requests must be responded to without delay and no later than a month after receipt of the request.

Right to Rectification

The data subject has the right to require a data controller to rectify any errors in their personal data. The response to the exercise of this right must be within a month of being notified of it.

If no action is being taken in response to the request, the data subject must be informed of this as well as their right to lodge a complaint with the Information Commissioner's Office.

Third parties to whom the personal data has been disclosed should also be informed of the exercise of this right.

Right to Erasure

The data subject has the right to require a data controller to delete their personal data if the continued processing of their data is not justified. This will involve consideration of whether the organisation has a lawful basis for processing the personal data.

Right to Restrict Processing

Data subjects may not be entitled to require the data controller to erase their personal data but may be entitled to limit the purposes for which the controller can process those data. This may occur where the accuracy of the data is contested, the processing is unlawful but the data subject requests restriction instead of deletion or where the data is no longer required by the data controller, but the data subject requires it for the establishment, exercise or defence of legal claims.

Right to Data Portability

The data subject has the right to transfer their personal data between controllers. This right may only be exercised where the legal foundation is consent or contract. It does not apply where the controller is acting under official authority on or in the public interest.

Data subjects have the right to receive personal data relating to them in a structured, commonly used, machine readable format to enable them to keep, use or share it with a third party or another controller. The right can be exercised by requesting one controller to provide it directly to another. The right only applies where the personal data is in electronic form.

Right to Object

A data controller must have a lawful basis for processing personal data. However, where that lawful basis is either “public interest” or “legitimate interests”, these lawful bases are not absolute, and data subjects may have a right to object to such processing. The right to object is a conditional right and can be refused if legitimate interests or public interest override the data subject’s rights or where the processing is for the establishment, exercise or defence of a legal claim.

Right to Not be Evaluated on the Basis of Automated Processing

Data subjects have the right not to be evaluated in any material sense solely on the basis of automated processing of their personal data.

Complaints

In addition to these rights, data subjects are entitled to lodge a complaint with the Information Commissioner’s Office if they are dissatisfied with the PCC’s compliance with the data protection regime.

10. Data Breaches

In the case of a personal data breach, the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Information Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay. The communication should include the nature of the breach and recommendations for mitigating adverse effects.

Any suspected personal data breach shall be notified to the Data Protection Officer without delay for consideration of action.

All personal data breaches shall be entered into the Data Breach Log created for this purpose (Appendix G).

11. Data Protection Officer

The PCC has designated the Chief Executive as the Data Protection Officer to take responsibility for data protection compliance within the OPCC.

The Data Protection Officer shall:

- keep the PCC and his staff abreast of their data protection obligations;
- monitor compliance with data protection obligations;
- ensure appropriate awareness-raising and training takes place;
- ensure compliance with data protection obligations is provided for from time to time under the internal audit programme;
- provide advice where requested;
- co-operate with the Information Commissioner's Office;
- act as the contact point for the Information Commissioner's Office.

Under the Scheme of Governance and Consent, the Head of Commissioning and Governance, the Head of Policy and Performance, and the Head of Communications and Engagement are authorised to deputise for the Chief Executive in his absence as required. This includes deputising for the Chief Executive in his role as Data Protection Officer.

12. Policy Review

The Chief Executive is authorised by the PCC to keep this policy and all elements of it under continuous review and to revise and reissue the policy as he considers necessary.

Appendix A: Basis for PCC Controlling and Processing Personal Data

1. **Appointments (and Applications for Appointment)**
    a. Chief Constable - Police Reform and Social Responsibility Act 2011, Section 38
    b. Audit Committee Members - The Financial Management Code of Practice for the Police Forces of England and Wales (Home Office, 2013)
    c. Legally Qualified People - Police (Conduct) Regulations 2020, Regulation 28
    d. Independent Members - Police (Conduct) Regulations 2020, Regulation 28
    e. Employees of the PCC - Police Reform and Social Responsibility Act 2011, Schedule, implied consent and contract.
    f. Custody Visitors - Police Reform Act 2002, Section 51

2. **Contacts**
    a. The Policing Protocol Order 2023 and consent

3. **Correspondents**
    a. The Policing Protocol Order 2023 and consent (where appropriate)

4. **Complainants**
    a. The Policing Protocol Order 2023 and consent (where appropriate)
    b. The Elected Local Policing Bodies (Complaints and Misconduct) Regulations 2012

5. **Complaints Review**
    a. The Police (Complaints and Misconduct) Regulations 2020
    b. The Police Reform Act 2002, Schedule 3

6. **Police Appeals Tribunals**
    a. Police Act 1996, Section 85 and Schedule 6, The Police Appeals Tribunals Rules 2020

7. **Miscellaneous Personal Data**
    a. Police Reform and Social Responsibility Act 2011
    b. The Policing Protocol Order 2023

Appendix B: General Data Protection Regulation (UK GDPR) Privacy Notice

Applications for Appointment

The Police and Crime Commissioner for Suffolk (PCC) is a data controller for the purposes of the UK GDPR. In the discharge of his statutory functions he of necessity collects personal data from data subjects.

The PCC in pursuance of his statutory functions makes appointments relating to the Chief Constable, the PCC's statutory officers, his employees, the Audit Committee, Legally Qualified People and Independent Members of Misconduct Panels and Custody Visitors.

In order to make these appointments he requires access to the personal data of applicants. The data collected in the application process will be used to make appointment decisions. In the case of unsuccessful applicants the data will be retained and disposed of in accordance with the time period specified in the PCC's UK GDPR Policy (available on the PCC website). Where an applicant is successful the applicant's data will be retained and disposed of, again in accordance with the time period in the UK GDPR policy.

Personal data obtained from successful applicants will be used to facilitate the successful delivery of the appointments. It will be shared with the Chief Constable and Suffolk Constabulary in order to deliver where appropriate the functions relating to service delivery, HR, pension, payroll, ICT and vetting and such other necessary functions.

Appropriate personal data such as contact data will also be shared within the functional groupings of appointees in order to facilitate the more efficient performance of the statutory functions requiring to be performed.

In the case of Legally Qualified People and Independent Members of the Eastern Region Panels, appropriate personal data will be shared with other Regional PCCs, Chief Constables and Constabularies.

Your personal data will only be reasonably used to enable the discharge of statutory functions. The PCC has adopted a UK GDPR Policy which sets out his approach to handling personal data. It is available through the PCC's website or alternatively a copy may be requested by contacting the PCC at the address below.

A data subject has the following rights under the UK GDPR:

- The right of access to their personal data;
- The right to require a controller to rectify errors in their personal data;
- The right to require a controller to delete their personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of their personal data;
- The right to transfer their personal data between controllers where appropriate;
- The right to object to the processing of their data in certain circumstances;
- The right not to be evaluated on the basis of automated processing;
- The right to make a complaint to the Information Commissioner's Office.

These rights are explored in more detail in the PCC's UK GDPR Policy.

The contact details for the PCC and/or the Data Protection Officer for the PCC are:

Police and Crime Commissioner for Suffolk
Police Headquarters Martlesham Heath
Ipswich
IP5 3QS

Tel: 01473 782773

Email: spcc@suffolk.pnn.police.uk

Web: www.suffolk-pcc.gov.uk

Appendix C: General Data Protection Regulation (UK GDPR) Privacy Notice and Consent

For use with Correspondents and Complainants

The Police and Crime Commissioner for Suffolk (PCC) is a data controller for the purposes of the UK GDPR. In the discharge of his statutory functions he of necessity collects personal data from data subjects.

The PCC in pursuance of his statutory functions receives and responds to correspondence from members of the public, and receives complaints about the Chief Constable, Constabulary, himself and others. This means that he will receive and process personal data relating to these data subjects.

In some instances in order to respond to correspondence and deal with complaints the PCC will need to pass that personal data on to a third party, such as the Chief Constable or the Constabulary, in order to obtain information to inform a response to the issue being raised. In these instances there is effectively a choice for a data subject as to whether a data subject's personal data is passed on to a third party. Clearly refusal to give consent to pass the data to a third party may prevent the PCC from giving or facilitating an informed response to a correspondent or complainant.

Accordingly in the case of correspondents and complainants the PCC seeks explicit consent to process their personal data to enable a response to be given and further, consent to share their personal data with a third party, as set out above, where appropriate, in order to facilitate or enable that response.

Your personal data will only be reasonably used for purposes of the PCC discharging his statutory functions. The PCC has adopted a UK GDPR Policy which sets out his approach to handling personal data. It is available through the PCC's website or alternatively a copy may be requested by contacting the PCC at the address below.

A data subject has the following rights under the UK GDPR:

- The right of access to their personal data;
- The right to require a controller to rectify errors in their personal data;
- The right to require a controller to delete their personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of their personal data;
- The right to transfer their personal data between controllers where appropriate;
- The right to object to the processing of their data in certain circumstances;
- The right not to be evaluated on the basis of automated processing;
- The right to make a complaint to the Information Commissioner's Office.

These rights are explored in more detail in the PCC's UK GDPR Policy.

The contact details for the PCC and/or the Data Protection Officer for the PCC are:

Police and Crime Commissioner for Suffolk
Police Headquarters Martlesham Heath
Ipswich
IP5 3QS

Tel: 01473 782773

Email: spcc@suffolk.pnn.police.uk

Web: www.suffolk-pcc.gov.uk

Before the PCC may exercise his responsibilities with you as a correspondent and/or complainant, please indicate in writing by email or letter to the PCC that you agree to the processing and sharing of your personal data as set out above.

If you choose, you may revoke your consent at any time in writing by letter or by email.

Appendix D: General Data Protection Regulation (UK GDPR) Privacy Notice and Consent

For use with Contacts

The Police and Crime Commissioner for Suffolk (PCC) is a data controller for the purposes of the UK GDPR. In the discharge of his statutory functions he of necessity collects personal data from data subjects.

The PCC in pursuance of his statutory functions collects the personal contact data of data subjects with whom he liaises for the purposes of governance, dissemination of information, public and business meetings, surveys and consultations.

The PCC seeks explicit consent from such data subjects to process their personal data as above. Your personal data will only be reasonably used for purposes of the PCC discharging his statutory functions.

The PCC has adopted a UK GDPR Policy which sets out his approach to handling personal data. It is available through the PCC's website or alternatively a copy may be requested by contacting the PCC at the address below.

A data subject has the following rights under the UK GDPR:

- The right of access to their personal data;
- The right to require a controller to rectify errors in their personal data;
- The right to require a controller to delete their personal data if the continued processing of those data is not justified;
- The right to restrict the controller in the processing of their personal data;
- The right to transfer their personal data between controllers where appropriate;
- The right to object to the processing of their data in certain circumstances;
- The right not to be evaluated on the basis of automated processing;
- The right to make a complaint to the Information Commissioner's Office.

These rights are explored in more detail in the PCC's UK GDPR Policy.

The contact details for the PCC and/or for the Data Protection Officer for the PCC are:

Police and Crime Commissioner for Suffolk
Police Headquarters Martlesham Heath
Ipswich
IP5 3QS

Tel: 01473 782773

Email: spcc@suffolk.pnn.police.uk

Web: www.suffolk-pcc.gov.uk

Before the PCC may exercise his responsibilities with you as a contact, please indicate in writing by email or letter to the PCC that you agree to the processing of your data for contact purposes as set out above. If you choose, you may revoke your consent at any time in writing by letter or by email.

Appendix E: Standard UK GDPR Conditions for Commissioning Awards

1. The grant recipient will, in relation to the service being commissioned, ensure that any data processing that is carried out to deliver the service meets the requirements of the General Data Protection Regulation or other relevant data protection legislation, and further ensure that the rights of the data subject are delivered.
2. The grant recipient will be expected to evidence their compliance as appropriate with the UK GDPR and such other relevant legislation if asked to do so by the PCC.

Appendix F: Data Asset Register / Retention Periods

1. Police and Crime Commissioner Business

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
SMT agendas and action logs		E		2 yrs	Business Need
Decisions (and associated papers) and decisions logs		E		Permanent	Statutory
Regional PCC meetings, Collaboration, Partnership and external meetings (where the PCC owns the record)		E		Permanent (reports) 6yrs (supporting documents) 6yrs (Q & A's)	Statutory
Regional PCC meetings, Collaboration, Partnership and external meetings (where the PCC does not own the record)		E		4 yrs	Statutory
PCC Planning & reporting: • Police and Crime Plan • Business Plans • Strategies and Policies • Annual Reports		E		Permanent	Statutory
Appointment of the Chief Constable		E and H		6 yrs (Advertisements) 1 yr (unsuccessful application forms) 6 yrs after last pension payment (Personnel files)	Statutory
Leaving of Chief Constable		H		6 yrs after termination or, if pension paid, 6 yrs after last pension payment.	Statutory

Complaints (all including those against Chief Constable and OPCC)		H and E		6 yrs	Statutory
Police Complaints Reviews		H and E		6 yrs	Statutory
Independent Custody Visiting Scheme: • Annual Report • Visitors report and Co-ordinator meeting notes • ICV Expenses • Custody Visitor details • Applications (unsuccessful) • Scheme Handbook		 H		 Permanent 6 yrs 6 yrs 2 yrs after end of appointment 1 yr Until Superseded.	Statutory
Freedom of Information (correspondence)		E		5 yrs from end of any appeal in relation to FOI	FOI Act 2000
Data Protection (subject access requests)		E		2 yrs	FOI Act 2000
Correspondence (members of the public)		E		2 yrs as of last correspondence on topic	Chief Constable's Retention Policy re Correspondence

2. Consultation, Engagement, Media and Public Relations

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Engagement strategies and correspondence		E		4 yrs	Business Need
Public Consultation (Strategy, records, correspondence, minutes and supporting papers)		E and H		4 yrs after collation	Statutory

Press Releases		E		4 yrs unless relating to an ongoing project	Business Need
Marketing • Developing and promoting of OPCC events • Information about the OPCC		E E		2 yrs Until superseded	Business Need
Independent Advisory Group (IAG) – disbanded in 2018		E		**NO LONGER EXISTS AND RETENTION PERIOD FOR ALL DATA HAS PASSED – DELETE ALL.**	

3. Police and Crime Commissioner

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
PCC expense claims		E and H		6 yrs	Chief Constable's Retention Policy
Register of Interests and Gifts & Hospitality		E and H		Permanent	Statutory
Code of Conduct		E and H		2yrs after office ends	Statutory
PCC Declaration		E and H		Permanent	Statutory
Contacts with whom PCC liaises		E		2 years from last contact	Reasonable period to assess whether further contact necessary

4. Office if the Police and Crime Commissioner Internal Management and Administration

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Governance Framework • Scheme of Governance • Delegation of Functions • Terms of Reference • Standing Orders/Financial Regulations		E and H		Permanent	Statutory
Constabulary Police Performance Monitoring • Monthly/Quarterly/Annual Statistics • PCC response to HMICFRS Reports • Internal Constabulary Performance meetings reports and statistics		E		5 yrs	Statutory
Accountability and Performance Panel • **Minutes, agendas, reports**		E		5 yrs	Statutory
Joint Audit Committee • Minutes, agendas, reports • Annual Audit Letter • External Audit Letter • Internal Audit Letter • Terms of Reference • Personnel files		E and H		6yrs	Statutory
Risk Register		E		2yrs after risk is mitigated	Statutory

5. Office of the Police and Crime Commissioner – Human Resources

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
OPCC Recruitment including Chief Executive, CFO, Monitoring Officer and s151 Officer • Application forms (unsuccessful) • Leavers • Completed vetting forms (unsuccessful) • Application forms (successful) and interview notes • Completed vetting forms (successful)		E and H		1yr 6yrs Immediately after end of process 4yrs Upon termination of employment	Statutory
OPCC staff/officers – HR records/personnel files • Performance reviews/training/grievances/appeals • Contracts • Accidents at work • Payroll • Pensions		E and H		6yrs from leaving date Until age 100	Chief Constable's Retention Policy generally on People
Policies and Procedures		E and H		Until Superseded	Statutory

6. Property and Land Management

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Insurance		E		7yrs after term expires	Statutory
Suffolk Estates Board • Minutes/agendas/reports		E		6yrs	In line with other minutes

7. Police and Crime Panel

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
PCC Scrutiny • Confirmation hearing paperwork • Complaints handling		E		6yrs	Statutory

8. Police and Crime Commissioner – legal and Contracts

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Litigation and Legal Advice • Correspondence • Criminal and civil case files		E and H		6yrs after last action (Litigation) 3yrs (Legal Advice)	Chief Constable's Retention Policy re Litigation
Service Level Agreements		E and H		6yrs after expiry	Statutory
Police Appeal Tribunals		E		6yrs	Reasonable period to assess

• Correspondence, reports, agendas, minutes, records of PAT cases etc					whether any need to retain for purposes of litigation.
Sealing Register		H		Permanent	Statutory
Asset Acquisition /Disposal • Legal documents relating to sale/purchase • Leases • Tender documents		E and H		6yrs (12 if over £50K) All deeds and supporting documents to be retained for five years after the disposal of property/land or the conclusion of any obligation or benefit to the PCC set out in the lease, whichever is later.	Business Need
Police Medical Appeals • Correspondence, reports, agendas, minutes, records of Appeals		E		6yrs	H&S at Work Act 1974

9. Finance

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Annual statement of accounts		H and E		Permanent	Statutory
Medium Term Financial Strategy		E		Until superseded and for 5yrs	Statutory
Treasury Management Strategy and Outturn report		E		1yr	Statutory
Asset Monitoring and maintenance • Asset Registers • Inventories and stocktaking		E		 Destroy after 7yrs after FY end Destroy after 2yrs	Business Need

• Acquisition and disposal reports				Destroy after sale or disposal	
OPCC Budget Setting • Final annual report • Draft budget and estimates • Budget monitoring		E		 Permanent 4yrs after budget set Destroy after following yrs budget set	Statutory
OPCC Expenditure • Invoices • Receipts • Bank statements • Vouchers • Ledgers • Write off of Public monies		E		7yrs after end of FY	Statutory
Funding agreements		E		7yrs	Statutory
Commissioning • Service provider reports • Specification, project documents and quotes • Contracts • Project Media (not PCC owned) • Partner's policy documents		E and H		 7yrs 7yrs 7yrs 2yrs 2yrs after contract end	Statutory and to meet HO and MoJ obligations.
Grants • Awarded • Not awarded • Received • Grant monitoring documents • Grant Variation documents		E		 7yrs 2yrs 7yrs 7yrs 7yrs	Statutory
Precept charges		E		6yrs plus current FY	Statutory

10. General

Description	Asset Owner	Format (Hard copy, Electronic)	Location	Retention Period (minimum)	Rationale
Independent Members – Misconduct Hearings, LQCs etc. • Appointment process • Expenses and Allowances		E		6yrs after leaving	Business Need

Appendix G – Data Breach Log

Date Data Protection Officer Norified	Details	Action Taken	Outcome of Referral to ICO where applicable and Date