OPCC Data Protection Policy

Document Approval and Identification

Author	Mike Richmond
Document can be reviewed by	Statutory Operations Manager
Document can be approved by	Chief Executive & Monitoring Officer
Document Title	OPCC Data Protection Policy
Version Number	2
Date	28/6/2022
Total Number of Pages	6
Security Marking	OFFICIAL

Version History

Version No.	Version Issue Date	Authored / Revision by	Approved by	Reason
2	**28/6/2022**	**Mike Richmond**	**Rachel Cook**	**Updated following APACE guidance**

The OPCC undertakes to handle information it holds about individuals in the appropriate manner. Procedures for the handling of such information will be compliant with the UK-GDPR and the Data Protection Act 2018.

Personal information will be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

The Data Protection Act does not guarantee personal privacy at all costs, but aims to strike a balance between the rights of individuals and the competing interests of those with legitimate reasons for using personal information.

We will make sure that:

- Information about individuals is only processed or shared for a business reason with a lawful purpose;
- Information is stored securely and is only accessed by authorised staff;
- Personal information is accurate and up to date;
- Information is destroyed once there is no further need for it;
- Staff are trained in their duties and responsibilities under the Data Protection Act
- The OPCC's notification (ref: TBC) to the Information Commissioner is up to date and reviewed annually.

Roles and Responsibilities

Senior Information Risk Owner (SIRO)

The Chief Executive Officer of the OPCC is the organisation's SIRO.

- The SIRO's role is to ensure information assets and risks within the organisation are **managed as a business process** rather than as a technical issue.
- The SIRO should be a champion of governance and must ensure there are **consistent and repeatable approaches** to managing risk at all levels of the organisation.
- The SIRO must **own the organisation's overall information management policy and risks and ensure they are implemented / mitigated consistently.**

Responsibilities:

The SIRO is responsible for:

- ensuring that the data protection legislation and policy is applied and maintained consistently throughout the organisation
- owning and reviewing information-based risks
- ensuring that DPIAs are carried out on all new projects when required
- understanding the information risks faced by the organisation, its partners and commissioned services ensuring that they are addressed, and that they inform strategic priorities
- ensuring that information risk assessment and mitigating actions taken benefit from an adequate level of independent scrutiny

Data Protection Officer (DPO)

The DPO assists the SIRO to monitor internal compliance, inform and advise the organisation on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the ICO.

Statutory Operations Manager

The Statutory Operations Manager is responsible for ensuring that the staff undertaking Freedom of Information (FOI) and Subject Access request comply with the law.

All Staff

All staff are required to read and comply with the organisations' data protection policies and seek the advice of the DPO where appropriate.

Subject Access Requests

The procedure for making a request for personal data will be published on our website as part of our Privacy Notice.

Third Party Information

If a request includes personal information about a third party, the information will only be disclosed if it will not breach any of the data protection principles. The key issues are fairness, lawfulness and the expectation of privacy.

Where a request is made for information about a person other than the applicant or the OPCC – or disclosure could affect the interests of a third party – the OPCC will consult the third party in order to determine if an exemption applies. The final decision will be made by the OPCC.

Consent

Where consent is relied upon as the lawful basis for processing personal data, a record will be kept of each person's consent. Periodic checks will be made that the consent is still valid, the frequency of which will depend upon the purpose of the processing and will be recorded in a DPIA.

Data subjects can withdraw their consent for processing at any time, at which point their data will be fully removed from the systems in questions at the earliest opportunity and no further processing of their personal data will be undertaken.

Data Protection Impact Assessments

Whenever we consider an activity that may include the processing of personal data, we will consider whether a Data Protection Impact Assessment (DPIA) is required. A DPIA will identify and mitigate any high risks to individuals.

A screening document will be completed in conjunction with the DPO that records the decision whether or not to conduct a full DPIA.

A DPIA will be completed if we plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.
- use new technologies;

- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- track individuals' location or behaviour;
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

Even if there is no specific indication of likely high risk, we will conduct a DPIA for any major new project involving the use of personal data.

Each DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.
- include a review date except for one-off activities.

The DPIA will be completed and logged by the Data Protection Officer in conjunction with the person leading on the project. It will be signed off by the DPO, with guidance being sought from the CEO where appropriate – for example in areas with high reputational risk or where new technology is being used.

If there are remaining areas of high risk to data subjects' rights and freedoms, the DPO will consult with the Information Commissioner's Office.

The results of the DPIA will be shared with any stakeholders that are consulted and DPIAs will be shared (redacted where appropriate) on the OPCC website.

Processing must not take place until mitigating measures are in place following the DPIA.

DPIA are to be reviewed regularly, based on risk, one year after implementation then at least every three years – or where the context or purpose of the processing changes.

Data Sharing

Information and knowledge are key corporate assets and we all have a responsibility to share and re-use them to release their value and maximise benefits to the business and the public. Data held by the organisation should be open to re-use unless there is a good reason not to.

When can data be shared internally?

Data should be shared internally by means of storage on searchable computer systems of clearly documented filing systems. Staff are encouraged to seek out and reuse existing datasets held by the organisation in preference to sourcing new data wherever feasible.

When can data be shared externally?

The organisation takes a responsible and risk-based approach to data sharing. Much of the information processed by the organisation may be shared with partners of the public. Wherever practicable, information in the public interest will be proactively published on the external website in a reusable format.

Special Provisions for Personal Data

Personal data shall only be internally shared and reused if the new purpose is compatible with that for which it was collected, a record will be kept of the reuse and the rationale behind it and, where required under the Data Protection Act 2018, the Data Subject(s) shall be informed of the new use wherever it is reasonably practicable to do so. If Special Category Personal Data is shared, the Data Protection Officer must first be consulted and a record kept of the lawful purpose for doing so.

Personal Data controlled by the organisation may only be shared with partner agencies after a risk-assessment has been undertaken by the Data Protection Officer in consultation with a member of the Senior Management Team (SMT). The risk assessment will establish a lawful basis for sharing and consider whether any of the data is personal data and consider any organisational or reputational risks to the organisation or its partners should the data be subject to a breach.

Ad-Hoc Information Sharing

Whenever personal data is shared with a partner agency, a record must be kept of:

- The date the information was shared
- What data was shared (e.g. names, email addresses)
- How much data was shared (e.g. number of records)
- Who it was shared with
- The lawful basis for sharing

This information will be sent to the Data Protection Officer by the person who shares the dat. A register of ad-hoc information sharing activity will be held.

Information Sharing Agreements

When information controlled by the organisation is to be shared automatically, systematically or regularly, an Information Sharing Agreement (ISA) should be considered. A record of Information Sharing Agreements will be held by the organisation and regular reviews by their owners will be

coordinated by the Data Protection Officer. ISAs are, by their nature, unique to each set of data and signatories, but a template is held by the Data Protection Officer which outlines the basic requirements.

Sharing under the lawful basis of Vital Interests

Where information is requested in order to protect life, and a legal basis of "Vital Interests" is established, relevant information will be shared as soon as reasonably practicable outside of the usual protocols. A retrospective risk-assessment will be completed by the person sharing in conjunction with the Data Protection Officer and full records will be kept of the information shared and the rationale.

Inaccurate or incomplete information

Where the organisation is made aware that shared personal data is inaccurate or complete, each recipient should be contacted to inform them about the rectification unless this is impossible or involves disproportionate effort.

Restriction of Processing

Where the organisation is advised of a potential inaccuracy then the personal data in question must be restricted. This will ordinarily be done by removing it from live systems and placing it temporarily in a restricted folder or removing it from the website until an assessment has been made. Each recipient should be contacted to inform them about the restriction unless this is impossible or involves disproportionate effort.

Freedom of Information

The Freedom of Information Act (FOIA) imposes a duty for a public body:

1. To confirm or deny that the information requested is held.
2. If the information is held, to communicate it to the applicant

Anyone may make a request for recorded information held by or on behalf of the Office of the Police and Crime Commissioner (OPCC). The OPCC must reply within 20 days unless an exemption applies.

Roles and Responsibilities

All staff are responsible for ensuring that any request for information they receive is dealt with in compliance with this policy. The Statutory Operations Manager coordinates all requests for information.

The CEO will act as the Qualified person in the event of a potential Section 36 exemption.

Publication Scheme

The OPCC maintains a publication scheme, listing the classes of information and the documents that it routinely publishes or intends to publish. The publication scheme will be on the OPCC website and reviewed as appropriate.

Handling and Tracking of Requests

The dedicated routes for valid information requests are:

- The email address pcc@humberside.pnn.police.uk
- By post to:
  Office of the Police and Crime Commissioner for Humberside

  The Lawns

  Harland Way

  Cottingham

  East Yorkshire

  HU16 5SN

All FOIA requests will be logged and tracked by the Statutory Operations Manager. This will aid identification of repeat, similar or vexatious requests and inform the development of the publication scheme.

Where there is reason to believe that some or all of the information requested is held by another public body, the OPCC will contact the applicant and, where possible, provide information about where to redirect the request. Under no circumstances will a person's request (and therefore their personal data) be forwarded direct to another organisation without their prior consent.

Exemptions and the Public Interest Test

There are 23 exemptions from the right of access. Eight are designated 'absolute', meaning that if one applies there is no further need to consider the request. The others are known as 'qualified' exemptions and require a public interest test to be applied. This considers whether the public interest in withholding the information outweighs the public interest in disclosing it.

Where an exemption is deemed to apply to some or all of the information requested, the applicant will be notified in writing. The relevant exemption will be cited, and any information that is not exempt will be provided.

Where a qualified exemption is being considered, the OPCC must conduct a public interest test to determine if it is in the public interest to release the information. The force FOI team may be consulted for an opinion.

In determining whether disclosure would be likely to prejudice the conduct of public affairs (Section 36 of the Act), the designate Qualified Person will decide on disclosure. If legal advice is thought to be necessary, it will be sought by the Chief Executive.

Fees

The OPCC will follow the Freedom of Information (Appropriate Limits and Fees) Regulations 2004. Accordingly all requests that cost less than £450 to process (the 'appropriate limit' – 18 hours at £25 per hour) will be complied with free of charge. Where we estimate that complying with a request would exceed the appropriate limit we will try to assist applicants to make a more refined request within the limit.

Information that is published under the Publication scheme will not be charged for.

Complaints

Anyone who has made a request for information to the OPCC under the FOIA is entitled to request an internal review if they are unhappy with the way their request has been handled. Internal reviews will be carried out by a senior member of staff who was not involved in the original decision. The internal review will consider whether the request was handled appropriately in line with the FOIA.

Applicants can make a request for an internal review within 40 days of the OPCC's response to their request. We will aim to respond to internal reviews within 15 working days of receipt.

If dissatisfied with the outcome of the internal review, the applicant may appeal to the Information Commissioner who has powers to uphold or overturn the decision.

Reporting of data security breaches to the ICO

This section provides guidance to The Office of the Police and Crime Commissioner for Humberside and a decision making process for notifying the Information Commissioner's Office (ICO) in the event of the loss, theft, unauthorised disclosure or compromise of personal data. It should be read in conjunction with the ICO's guidance on notifying data security breaches.

Authority Levels

The decision whether or not to report a data breach will be made by the Data Protection and Disclosure Officer or, in their absence the Statutory Operations Manager or Chief Executive Officer.

Definitions

'Personal data' is information which can identify a living individual. This can include information that, when combined with other readily available information, can identify a living individual.

The GDPR defines a *'personal data breach*' as:

> *"…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".*

This includes breaches that are the result of accidental or deliberate causes. It also makes clear that a breach is not just about the *loss* of personal data. Anything that affects the **confidentiality**, **availability** or **integrity** of personal data constitutes a breach.

Legal Requirements

The use of personal data is governed by the principles set out in the Data Protection Act 2018. Under the Act all data controllers have a responsibility to ensure appropriate and proportionate security of the personal data they hold. There is a legal obligation to report certain breaches of security which result in the loss, theft, unauthorised disclosure or compromise of personal data within 72 hours of their discovery.

Identification of a Data Breach

Any member of OPCC staff who discovers or has reasonable grounds to suspect that a breach of personal data has occurred **must** inform either the Data Protection Officer, Statutory Operations Manager or Chief Executive Officer at the earliest possible opportunity.

If a loss, theft, unauthorised disclosure or compromise of non-personal data occurs then it will not be necessary to consider whether or not to notify the ICO but the DPO still must be informed.

Rights of Data Subjects

Any individual who becomes aware of the loss of their own or someone else's personal data can make a complaint directly to the Information Commissioner. Any such complaint will normally trigger an investigation by the ICO. Whether or not the incident had already been reported by the organisation involved would normally be considered by the investigators and the subsequent judgement.

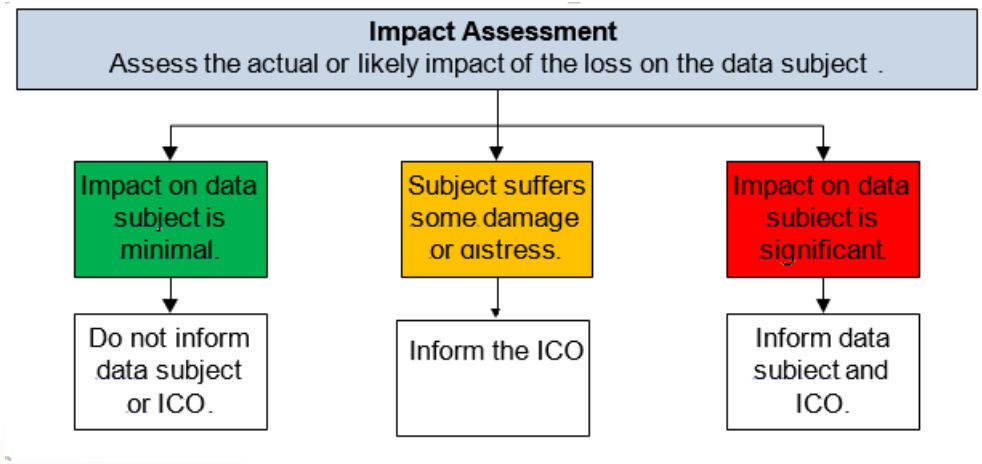
Risk Assessment process

The ICO must be informed where a data breach results (or could result) in a risk to one or more individuals' rights or freedoms. The following guidance provides a framework for assessing whether the ICO should be informed. It is not exhaustive, and only indicates the type of factors that may indicate the risks associated with a breach.

Notification Matrix

The Notification Matrix (Appendix A) will be used in conjunction with the Impact Assessment flowchart to determine whether a loss, theft, unauthorised disclosure or compromise of personal data should be reported to the ICO. Although not every breach will be reported, every breach will be recorded by the DPO. If there any doubt then the presumption will be to report the breach to the ICO.

Impact Assessment Flowchart



Timing Of Notification

If the outcome is to notify the ICO of the data protection breach, consideration must be given as to when to notify. Ordinarily notification should occur as soon as the information required for notification is available (information about what is required is listed in Appendix B) and in any case within 72 hours of discovery of the breach.

What Information must be provided to the ICO?

When reporting a breach, the following must be provided:

- a description of the nature of the personal data breach including, where possible:
  - the categories and approximate number of individuals concerned; and
  - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

What Information Must be provided to individuals?

The ICO guidance will dictate when individuals are to be informed about a data breach.

- DPO's details
- Details of the data that was breached
- A description of the likely consequences and how to protect themselves
- Mitigation actions that have been put in place and possible adverse effects