

**Date:** 11/03/2026  
**Our ref:** 01/FOI/26/016305/F

**FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/26/016305/F**

I write in connection with your request for information dated 04/02/2026, received by Greater Manchester Police (GMP) for the following information:

***This request relates to Greater Manchester Police policies, training, and instructions given to staff regarding Subject Access Requests under data protection law and complaints made under the Police Reform Act 2002, specifically in relation to verbal requests and complaints and the practice of directing members of the public to online systems.***

***Please provide copies of the following information held by Greater Manchester Police.***

***1.***

***All training materials, guidance documents, manuals, scripts, internal policies, or written instructions used to train staff on handling Subject Access Requests under the UK GDPR and Data Protection Act 2018.***

***2.***

***All training materials, guidance documents, manuals, scripts, internal policies, or written instructions used to train staff on handling complaints under the Police Reform Act 2002.***

***3.***

***Any guidance, scripts, or instructions provided to call handlers, front desk staff, contact centre staff, or other staff who deal with the public by telephone in relation to Subject Access Requests and police complaints, including what staff are instructed to tell members of the public about how a SAR or complaint can be made.***

***4.***

***Any documents, policies, or guidance that state or imply that a Subject Access Request or a police complaint must be made online, or that direct staff to tell members of the public to use a website or online form to submit a SAR or complaint.***

***5.***

***Any internal documents or guidance that explain whether a Subject Access Request or a police complaint can be made verbally, including by telephone, and how staff are instructed to handle such verbal requests or complaints.***

6.

***Any training updates, internal communications, emails, or notices issued to staff in the last five years relating to incorrect or misleading information being given to the public about how to make a Subject Access Request or a police complaint.***

7.

***Any guidance or policy documents relating to identity verification for Subject Access Requests made verbally or by telephone, including whether identification is required at the point of request or can be provided after the request has been made.***

8.

***Any guidance or policy documents relating to circumstances in which staff are permitted to refuse to accept a Subject Access Request or a police complaint by telephone, including the legal basis relied upon for any such refusal.***

9.

***Any internal reviews, audits, or assessments conducted in the last five years relating to accessibility of Subject Access Requests and police complaints, including issues relating to verbal requests, telephone handling, or members of the public being directed to online systems.***

***\*\*\*\*\*To clarify, where my FOI refers to “complaints”, this is intended to cover complaints made by members of the public to Greater Manchester Police under the Police Reform Act 2002 in general, not subject access requests or data protection complaints.***

### **Result of Searches**

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP.

I am not obliged to supply you with all the information as an exemption applies.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because this information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies. The information you have requested is exempt from disclosure by virtue of the following exemption: Section 40(2) – Personal Information.

Where redactions occur in the attached documents, this represents information that identifies a living individual, to disclose this information would breach the principles of the GDPR and the Data Protection Act 2018. Personal data is defined by Article 4 of the GDPR and Part 1 of the Data Protection Act 2018 and means any information relating to an identified or identifiable natural person ('data subject'). An identified natural person is one who can be identified directly or indirectly from that data.

1. Please see the attached training document - To confirm, these are not formal GMP SAR training material. These are slides created by mentors/training coaches. Most of this information is also available via the ICO website.
2. All complaints by members of the public are directed to the GMP complaint portal via the GMP website where applicable. All complaints are handled by GMP's PSD in line with the COP - [Complaints and misconduct | College of Policing](#)
3. No policy is held in a recorded form to advise Call handlers on what to do when a subject access request comes through – Instead for Subject access and complaints, callers are directed to GMP's Single online Portal. - [Contact us | Greater Manchester Police](#) – See attachment also to support this
4. No information held – Please note Under Data Protection legislation, and validated in the ICO guidelines, SARs can be requested verbally. However, to ensure absolute clarity, and auditable content for the benefit of the applicant and the organisation, we do try to ask applicants where possible, that they submit their request via the GMP website portal, so they can fully explain what their request is and also provide the required ID documentation needed



for it to be a valid SAR. Applicants can and do also email our central subject access mailbox with their requests and ID also.

5. Please see the information provided online which is followed in line with the complaints handling process. [How to complain about the police | Greater Manchester Police](#)
6. No information held
7. See page 78 from Introduction to SARS training document. GMP also adhere to the ICO guidance on requesting ID - [What to expect after making a subject access request | ICO](#). You can make a subject access request to GMP, however before this can be officially logged our admins must verify your identity. It is advisable to submit this at the time of making any request, however GMP can ask for this after the request has been received.
8. Please see the attached redacted documents outlining the guidance provided to all GMP staff, call takers, officers and the GMCA.
9. Please see the attached redacted documents outlining the guidance provided to all GMP staff, call takers, officers and the GMCA.

**From:** [REDACTED]  
**To:** [REDACTED]  
**Subject:** PSD Responsibility for Single Online Home  
**Date:** 11 September 2024 13:47:00

---

Hi [REDACTED]

I am not sure if you are aware or not, I know certainly that members of your team will be aware as PS [REDACTED] from my team has been making some enquiries with your team as part of the testing she has undertaken before we have reached this point.

In summary from 0700hrs on Tuesday 17<sup>th</sup> September 2024 the PSD will take on full responsibility for Single Online Home (SOH). We will arrange for IT to divert them to a new email address which we have created.

We will be responsible for reviewing each complaint reported via SOH, recording it and deciding on the most appropriate handling giving consideration to the Complaints and Misconduct Regulations.

Of note the existing longstanding [REDACTED] address will be decommissioned as of the same date and time. This will instead make way for our new email address which will be [REDACTED]

The PSD WILL NO longer accept complaints from members of the public emailed in and I would ask that the new email address is not disclosed to members of the public to avoid any further dissatisfaction.

I would ask that the following is adhered to by your call takers

Any member of the public wishing to make a new complaint should be directed to SOH via the following link [Complaints | Greater Manchester Police \(gmp.police.uk\)](https://gmp.police.uk/complaints)

Any member of the public wishing to raise further dissatisfaction relating to a previously made complaint (ie they were told someone would be in contact and they haven't been contacted) they should be directed to SOH via the same link and asked to make a complaint (it then asks does your complaint relate to a previously reported complaint and the answer will be yes)

The call taker MUST NOT be tempted to send an email on behalf of the complainant to the PSD.

The [REDACTED] email address is where the SOH complaints will be sent to in addition to those that come via the IOPC.

If you have a member of the public who has additional needs and for example has no access to internet the options are that your call taker completes the SOH complaint for them or they record an incident and arrange for a district Inspector to make contact (similar to what happens now)

In the event a member of the public emails in to the new PSD email address they will receive an auto response sign posting them to SOH and advised their email will not be reviewed or

responded to this is why it is really important the public are not advised to contact the PSD directly.

From an internal referral perspective relating to anything other than complaints ie if you have concerns with regards to a member of staff from a conduct perspective these matters should be brought to the attention of your branch standards manager endorsed on a conduct referral form and can be referred in to [REDACTED]

Similarly any matter relating to a death or serious injury can also be sent in to this address.

I am arranging for some comms to be placed on the intranet and the website will be updated but if you could circulate within your branch to ensure compliance I would be most grateful.

Any questions as ever please let me know.

Regards

[REDACTED]

[REDACTED] | Detective Chief Inspector | Professional Standards Directorate

Mobile [REDACTED]

[REDACTED]

GSC: Official (unless otherwise stated)

PSD new mailbox

 PSD new mailbox

## Professional Standards Directorate (PSD)

We are excited to announce some major changes in how to contact the Professional Standards Directorate Complaints and Misconduct Unit.

### Public Complaints

From 7am on Tuesday 17 September 2024, external complaints made via the force's single online home will be referred directly to the Complaints and Misconduct Unit. At the same time the [REDACTED] mailbox will be retired. As an interim measure an automated response will be sent to any individual attempting to contact PSD via this mailbox.

All complaints taken in person by a police officer or member of police staff should be recorded on the expression of dissatisfaction form and sent to PSD via the new mailbox [REDACTED]

To ensure the consistent, effective and timely handling of all public complaints this new email address must not be disclosed to the public and instead the public are encouraged to raise their dissatisfaction via single online home portal which will enable an improved level of service.

[Make a complaint about the police | Greater Manchester Police \(gmp.police.uk\)](#)

Those with accessibility requirements can continue to make complaints via 101, at their local police station, or in writing. Those with hearing or speech impairments can use our textphone service – 18001 101.

External complaints can continue to be made via third parties including, the Local Policing Body – Greater Manchester Combined Authority (GMCA), and The Independent Office for Police Conduct (IOPC).

From the 'Go Live' date, the PSD will no longer accept complaints from members of the public submitted via email. Therefore, to avoid any further dissatisfaction you must not share the new email address with members of the public. The new mailbox is for INTERNAL USE ONLY.

**Misconduct and Death or Serious Injury (DSI)**

Any internal referral to PSD that is not a public complaint should be made via the new mailbox:

Standards Managers around the force have been made aware of the change. Their role remains key in maintaining high standards of reporting such matters to PSD. Serious matters should continue to be raised directly with the duty PSD Detective Inspector at the soonest opportunity.

This mailbox has been created to accommodate all internal referrals for conduct and death or serious injury (DSI) matters. This mailbox is for internal use only and should not be shared with the general public.

#### **Anonymous Reporting and ACU**

The contact details for the Anti-Corruption Unit also remain the same.

For any further information about referrals to PSD contact Detective Chief Inspector [REDACTED]



The poster features the Greater Manchester Police crest and logo at the top left, with the text 'GREATER MANCHESTER POLICE' and 'Professional Standards Directorate' to its right. Below this, it states 'New Mailbox from 0700 17, September 2024'. The main heading is 'Complaints and Misconduct Unit:', followed by 'Public complaints mailbox:' and a large redacted area. To the right of this area is a vertical box with the text 'For Internal Use Only'. Below the redacted area is the heading 'Anti-Corruption Unit:' followed by another redacted area. Further down is the heading 'Out of hours referrals:' followed by a paragraph of text: 'Enquiries between 1500-2300 Monday to Friday and weekend cover between 0700-2300 please refer to [REDACTED] the duty cover officer. They can be contacted via their mobile. Between 2300-0700 please contact the Detective Inspector on duty cover also listed on the MI [REDACTED] This information is also available via the Force Daily Summary and the Force Weekend Pack.' At the bottom, there is a section titled 'Misconduct Know someone breaking rules or procedures?' with a redacted area below it. In the bottom right corner, there is a graphic of a smartphone displaying the 'Police Integrity Line' app, with the text 'Police Integrity Line' and 'Download' below it.

**GREATER MANCHESTER POLICE** Professional Standards Directorate

*New Mailbox from 0700 17, September 2024*

**Complaints and Misconduct Unit:**  
Public complaints mailbox:  
[REDACTED] **For Internal Use Only**

**Anti-Corruption Unit:**  
[REDACTED]

**Out of hours referrals:**  
Enquiries between 1500-2300 Monday to Friday and weekend cover between 0700-2300 please refer to [REDACTED] the duty cover officer. They can be contacted via their mobile. Between 2300-0700 please contact the Detective Inspector on duty cover also listed on the MI [REDACTED] This information is also available via the Force Daily Summary and the Force Weekend Pack.

**Misconduct**  
Know someone breaking rules or procedures?  
[REDACTED]

**Police Integrity Line**  
Download

# Introduction to Data Protection, UK GDPR & SARs

Information Access Caseworker





# The Data Protection Act 2018 / UK GDPR

- The UK GDPR sets out seven key principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability
- These principles should lie at the heart of your approach to processing personal data.

# What are the Principles?

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime.

Article 5(1) requires that personal data shall be:

- “ (a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) 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, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

# Why are the Principles important?

The principles lie at the heart of the UK GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of the UK GDPR.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to £17.5 million, or 4% of your total worldwide annual turnover, whichever is higher.

# Principle(a) – Lawfulness, fairness & transparency

## At a glance

- You must identify valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data.
- You must ensure that you do not do anything with the data in breach of any other laws.
- You must use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned.
- You must be clear, open and honest with people from the start about how you will use their personal data.

## What is lawfulness?

For processing of personal data to be lawful, you need to identify specific grounds for the processing. This is called a 'lawful basis' for processing, and there are six options which depend on your purpose and your relationship with the individual. There are also specific additional conditions for processing some especially sensitive types of data. For more information, see the [lawful basis section of this guide](#).

If no lawful basis applies then your processing will be unlawful and in breach of this principle.



# Principle(a) – Lawfulness, fairness & transparency

Lawfulness also means that you don't do anything with the personal data which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If processing involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

These are just examples, and this list is not exhaustive. You may need to take your own legal advice on other relevant legal requirements.

Although processing personal data in breach of copyright or industry regulations (for example) will involve unlawful processing in breach of this principle, this does not mean that the ICO can pursue allegations which are primarily about breaches of copyright, financial regulations or other laws outside our remit and expertise as data protection regulator. In this situation there are likely to be other legal or regulatory routes of redress where the issues can be considered in a more appropriate forum.

If you have processed personal data unlawfully, the UK GDPR gives individuals the right to erase that data or restrict your processing of it.

# Principle(a) – Lawfulness, fairness & transparency

## What is fairness?

Processing of personal data must always be fair as well as lawful. If any aspect of your processing is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.

Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.

Personal data may sometimes be used in a way that negatively affects an individual without this necessarily being unfair. What matters is whether or not such detriment is justified.



# Principle(a) – Lawfulness, fairness & transparency



## **Example**

Where personal data is collected to assess tax liability or to impose a fine for breaking the speed limit, the information is being used in a way that may cause detriment to the individuals concerned, but the proper use of personal data for these purposes will not be unfair.

You should also ensure that you treat individuals fairly when they seek to exercise their rights over their data. This ties in with your obligation to facilitate the exercise of individuals' rights. Read our guidance on rights for more information.

# Principle(a) – Lawfulness, fairness & transparency

## What is transparency?

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data.

Transparency is always important, but especially in situations where individuals have a choice about whether they wish to enter into a relationship with you. If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship.

Transparency is important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important - as individuals may have no idea that you are collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'.

You must ensure that you tell individuals about your processing in a way that is easily accessible and easy to understand. You must use clear and plain language.

# Principle(b) – Purpose Limitation

## At a glance

- You must be clear about what your purposes for processing are from the start.
- You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.
- You can only use the personal data for a new purpose if either this is compatible with your original purpose, you get consent, or you have a clear obligation or function set out in law.

What is the purpose limitation principle?

Article 5(1)(b) says:

“

1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.”

# Principle(b) – Purpose Limitation

In practice, this means that you must:

- be clear from the outset why you are collecting personal data and what you intend to do with it;
- comply with your documentation obligations to specify your purposes;
- comply with your transparency obligations to inform individuals about your purposes; and
- ensure that if you plan to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

## Why do we need to specify our purposes?

This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned.

Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid 'function creep'. It also helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to building public trust in how you use personal data.

# Principle(b) – Purpose Limitation

There are clear links with other principles – in particular, the fairness, lawfulness and transparency principle. Being clear about why you are processing personal data will help you to ensure your processing is fair, lawful and transparent. And if you use data for unfair, unlawful or 'invisible' reasons, it's likely to be a breach of both principles.

Specifying your purposes is necessary to comply with your accountability obligations.

## How do we specify our purposes?

If you comply with your documentation and transparency obligations, you are likely to comply with the requirement to specify your purposes without doing anything more:

- You need to specify your purpose or purposes for processing personal data within the documentation you are required to keep as part of your records of processing (documentation) obligations under Article 30.
- You also need to specify your purposes in your privacy information for individuals.

However, you should also remember that whatever you document, and whatever you tell people, this cannot make fundamentally unfair processing fair and lawful.



# Principle(b) – Purpose Limitation

If you are a small organisation and you are exempt from some documentation requirements, you may not need to formally document all of your purposes to comply with the purpose limitation principle. Listing your purposes in the privacy information you provide to individuals will be enough. However, it is still good practice to document all of your purposes. For more information, read our [documentation guidance](#).

If you have not provided privacy information because you are only using personal data for an obvious purpose that individuals already know about, the “specified purpose” should be taken to be the obvious purpose.

You should regularly review your processing, documentation and privacy information to check that your purposes have not evolved over time beyond those you originally specified (‘function creep’).



# Principle(b) – Purpose Limitation

Once we collect personal data for a specified purpose, can we use it for other purposes?

The UK GDPR does not ban this altogether, but there are restrictions. In essence, if your purposes change over time or you want to use data for a new purpose which you did not originally anticipate, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

All processing must also be lawful, so you do need a lawful basis. The original basis you used to collect the data may not always be appropriate for your new use of that data.

If your new purpose is compatible, and your use of the data is necessary for that purpose, you can generally be confident it will also be lawful. In most cases, the appropriate basis for your new use of the data is likely to be fairly obvious. See our [lawful basis guidance](#) for more information.

However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful. See our [lawful basis guidance](#) for more information.

# Principle(b) – Purpose Limitation

Once we collect personal data for a specified purpose, can we use it for other purposes?

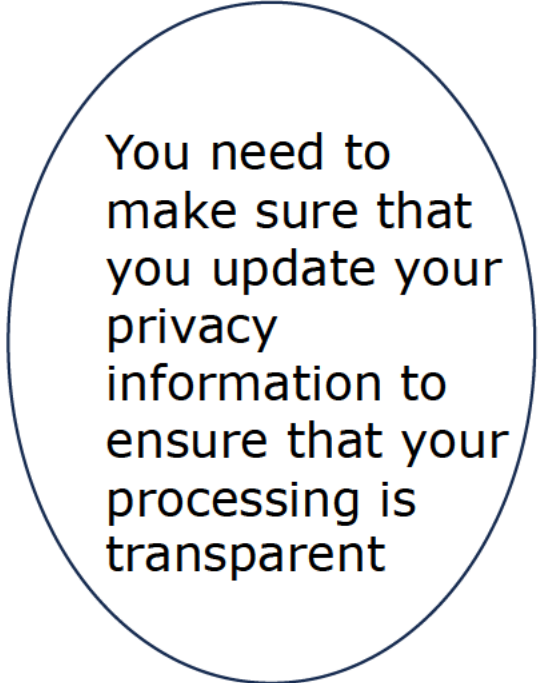
The UK GDPR does not ban this altogether, but there are restrictions. In essence, if your purposes change over time or you want to use data for a new purpose which you did not originally anticipate, you can only go ahead if:

- the new purpose is compatible with the original purpose;
- you get the individual's specific consent for the new purpose; or
- you can point to a clear legal provision requiring or allowing the new processing in the public interest – for example, a new function for a public authority.

All processing must also be lawful, so you do need a lawful basis. The original basis you used to collect the data may not always be appropriate for your new use of that data.

If your new purpose is compatible, and your use of the data is necessary for that purpose, you can generally be confident it will also be lawful. In most cases, the appropriate basis for your new use of the data is likely to be fairly obvious. See our [lawful basis guidance](#) for more information.

However, you should remember that if you originally collected the data on the basis of consent, you usually need to get fresh consent to ensure your new processing is fair and lawful. See our [lawful basis guidance](#) for more information.



You need to make sure that you update your privacy information to ensure that your processing is transparent

# Principle(b) – Purpose Limitation

What is a 'compatible' purpose?

The UK GDPR specifically says that the following purposes should be considered to be compatible purposes:

- archiving purposes in the public interest;
- scientific or historical research purposes; and
- statistical purposes.

Please read our [detailed guidance on the research provisions](#) for more information.

Otherwise, you need to do a compatibility assessment to decide whether a new purpose is compatible with your original purpose. The assessment should take into account:

- any link between your original purpose and the new purpose;
- the context in which you originally collected the personal data – in particular, your relationship with the individual and what they would reasonably expect;
- the nature of the personal data – eg is it particularly sensitive;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg encryption or pseudonymisation.

This list is not exhaustive and what you need to look at depends on the particular circumstances.

# Principle(b) – Purpose Limitation

We consider a compatibility assessment is likely to look at similar factors to a legitimate interests assessment (LIA). Although there's no requirement to do so, you could therefore use our [LIA template](#) to help you assess compatibility.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose data for this type of purpose.



## Example

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

# Principle(b) – Purpose Limitation

We consider a compatibility assessment is likely to look at similar factors to a legitimate interests assessment (LIA). Although there's no requirement to do so, you could therefore use our [LIA template](#) to help you assess compatibility.

As a general rule, if the new purpose is either very different from the original purpose, would be unexpected, or would have an unjustified impact on the individual, it is likely to be incompatible with your original purpose. In practice, you are likely to need to ask for specific consent to use or disclose data for this type of purpose.



## **Example**

A GP discloses his patient list to his wife, who runs a travel agency, so that she can offer special holiday deals to patients needing recuperation. Disclosing the information for this purpose would be incompatible with the purposes for which it was obtained.

# Principle (c) – Data Minimisation

## At a glance

You must ensure the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

## Checklist

- ☐ We only collect personal data we actually need for our specified purposes.
- ☐ We have sufficient personal data to properly fulfil those purposes.
- ☐ We periodically review the data we hold, and delete anything we don't need.



# Principle (c) – Data Minimisation

What is the data minimisation principle?

Article 5(1)(c) says:

“

1. Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)”

So you should identify the minimum amount of personal data you need to fulfil your purpose. You should hold that much information, but no more.

This is the first of three principles about data standards, along with accuracy and storage limitation.

The accountability principle means that you need to be able to demonstrate that you have appropriate processes to ensure that you only collect and hold the personal data you need.

Also bear in mind that the UK GDPR says individuals have the right to complete any incomplete data which is inadequate for your purpose, under the right to rectification. They also have right to get you to delete any data that is not necessary for your purpose, under the right to erasure (right to be forgotten).

# Principle (c) – Data Minimisation

How do we decide what is adequate, relevant and limited?

The UK GDPR does not define these terms. Clearly, though, this will depend on your specified purpose for collecting and using the personal data. It may also differ from one individual to another.

So, to assess whether you are holding the right amount of personal data, you must first be clear about why you need it.

For special category data or criminal offence data, it is particularly important to make sure you collect and retain only the minimum amount of information.

You may need to consider this separately for each individual, or for each group of individuals sharing relevant characteristics. You should in particular consider any specific factors that an individual brings to your attention – for example, as part of an objection, request for rectification of incomplete data, or request for erasure of unnecessary data.

You should periodically review your processing to check that the personal data you hold is still relevant and adequate for your purposes, and delete anything you no longer need. This is closely linked with the storage limitation principle.

# Principle (c) – Data Minimisation

When could we be processing too much personal data?

You should not have more personal data than you need to achieve your purpose.  
Nor should the data include irrelevant details.



## Example

A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are discounted. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

If you need to process particular information about certain individuals only, you should collect it just for those individuals – the information is likely to be excessive and irrelevant in relation to other people.



## Example

A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job.

# Principle (c) – Data Minimisation

You must not collect personal data on the off-chance that it might be useful in the future. However, you may be able to hold information for a foreseeable event that may never occur if you can justify it.



## Example

An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.

If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work.

If you are holding more data than is actually necessary for your purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach of the data minimisation principle. Individuals will also have the right to erasure.

# Principle (c) – Data Minimisation

When could we be processing inadequate personal data?

If the processing you carry out is not helping you to achieve your purpose then the personal data you have is probably inadequate. You should not process personal data if it is insufficient for its intended purpose.

In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question.



## Example

A group of individuals set up a club. At the outset the club has only a handful of members, who all know each other, and the club's activities are administered using only basic information about the members' names and email addresses. The club proves to be very popular and its membership grows rapidly. It becomes necessary to collect additional information about members so that the club can identify them properly, and so that it can keep track of their membership status, subscription payments etc.

Data may also be inadequate if you are making decisions about someone based on an incomplete understanding of the facts. In particular, if an individual asks you to supplement incomplete data under their right to rectification, this could indicate that the data might be inadequate for your purpose.

Obviously it makes no business sense to have inadequate personal data – but you must be careful not to go too far the other way and collect more than you need.



# Principle (c) – Data Minimisation

What about the adequacy and relevance of opinions?

A record of an opinion is not necessarily inadequate or irrelevant personal data just because the individual disagrees with it or thinks it has not taken account of information they think is important.

However, in order to be adequate, your records should make clear that it is opinion rather than fact. The record of the opinion (or of the context it is held in) should also contain enough information to enable a reader to interpret it correctly. For example, it should state the date and the author's name and position.

If an opinion is likely to be controversial or very sensitive, or if it will have a significant impact when used or disclosed, it is even more important to state the circumstances or the evidence it is based on. If a record contains an opinion that summarises more detailed records held elsewhere, you should make this clear.



## **Example**

A GP's record may hold only a letter from a consultant and it will be the hospital file that contains greater detail. In this case, the record of the consultant's opinion should contain enough information to enable detailed records to be traced.



# Principle (d) – Accuracy

## At a glance

- You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact.
- You may need to keep the personal data updated, although this will depend on what you are using it for.
- If you discover that personal data is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.
- You must carefully consider any challenges to the accuracy of personal data.

## What is the accuracy principle?

Article 5(1)(d) of the UK GDPR says:

“

1. Personal data shall be:

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')”

# Principle (d) – Accuracy

This is the second of three principles about data standards, along with data minimisation and storage limitation.

There are clear links here to the [right to rectification](#), which gives individuals the right to have inaccurate personal data corrected.

In practice, this means that you must:

- take reasonable steps to ensure the accuracy of any personal data;
- ensure that the source and status of personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically update the information.

## When is personal data ‘accurate’ or ‘inaccurate’?

The UK GDPR does not define the word ‘accurate’. However, the Data Protection Act 2018 does say that ‘inaccurate’ means “incorrect or misleading as to any matter of fact”. It will usually be obvious whether personal data is accurate.

You must always be clear about what you intend the record of the personal data to show. What you use it for may affect whether it is accurate or not. For example, just because personal data has changed doesn’t mean that a historical record is inaccurate – but you must be clear that it is a historical record.

# Principle (d) – Accuracy



## Example

If an individual moves house from London to Manchester a record saying that they currently live in London will obviously be inaccurate. However a record saying that the individual once lived in London remains accurate, even though they no longer live there.



## Example

The Postcode Address File (PAF) contains UK property postal addresses. It is structured to reflect the way the Royal Mail delivers post. So it is common for someone to have a postal address linked to a town in one county (eg Stoke-on-Trent in Staffordshire) even if they actually live in another county (eg Cheshire) and pay council tax to that council. The PAF file is not intended to accurately reflect county boundaries.

# Principle (d) – Accuracy

What about records of mistakes?

There is often confusion about whether it is appropriate to keep records of things that happened which should not have happened. Individuals understandably do not want their records to be tarnished by, for example, a penalty or other charge that was later cancelled or refunded.

However, you may legitimately need your records to accurately reflect the order of events – in this example, that a charge was imposed, but later cancelled or refunded. Keeping a record of the mistake and its correction might also be in the individual's best interests.



## **Example**

A misdiagnosis of a medical condition continues to be held as part of a patient's medical records even after the diagnosis is corrected, because it is relevant for the purpose of explaining treatment given to the patient, or for other health problems.

It is acceptable to keep records of mistakes, provided those records are not misleading about the facts. You may need to add a note to make clear that a mistake was made.

# Principle (d) – Accuracy



## Example

An individual finds that, because of an error, their account with their existing energy supplier has been closed and an account opened with a new supplier. Understandably aggrieved, they believe the original account should be reinstated and no record kept of the unauthorised transfer. Although this reaction is understandable, if their existing supplier did close their account, and another supplier opened a new account, then records reflecting what actually happened will be accurate. In such cases it makes sense to ensure that the record clearly shows that an error occurred.



## Example

An individual is dismissed for alleged misconduct. An Employment Tribunal finds that the dismissal was unfair and the individual is reinstated. The individual demands that the employer deletes all references to misconduct. However, the record of the dismissal is accurate. The Tribunal's decision was that the employee should not have been dismissed on those grounds. The employer should ensure its records reflect this.

# Principle (d) – Accuracy

## What about accuracy of opinions?

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact.

However, in order to be accurate, your records must make clear that it is an opinion, and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.



### **Example**

An area of particular sensitivity is medical opinion, where doctors routinely record their opinions about possible diagnoses. It is often impossible to conclude with certainty, perhaps until time has passed or tests have been done, whether a patient is suffering from a particular condition. An initial diagnosis (which is an informed opinion) may prove to be incorrect after more extensive examination or further tests. However, if the patient's records reflect the doctor's diagnosis at the time, the records are not inaccurate, because they accurately reflect that doctor's opinion at a particular time. Moreover, the record of the doctor's initial diagnosis may help those treating the patient later, and in data protection terms is required in order to comply with the 'adequacy' element of the data minimisation principle.



# Principle (d) – Accuracy

If an individual challenges the accuracy of an opinion, it is good practice to add a note recording the challenge and the reasons behind it.

How much weight is actually placed on an opinion is likely to depend on the experience and reliability of the person whose opinion it is, and what they base their opinion on. An opinion formed during a brief meeting will probably be given less weight than one derived from considerable dealings with the individual. However, this is not really an issue of accuracy. Instead, you need to consider whether the personal data is “adequate” for your purposes, in line with the data minimisation principle.

Note that some records that may appear to be opinions do not contain an opinion at all. For example, many financial institutions use credit scores to help them decide whether to provide credit. A credit score is a number that summarises the historical credit information on a credit report and provides a numerical predictor of the risk involved in granting an individual credit. Credit scores are based on a statistical analysis of individuals’ personal data, rather than on a subjective opinion about their creditworthiness. However, you must ensure the accuracy (and adequacy) of the underlying data.

# Principle (d) – Accuracy

Does personal data always have to be up to date?

This depends on what you use the information for. If you use the information for a purpose that relies on it remaining current, you should keep it up to date. For example, you should update your employee payroll records when there is a pay rise. Similarly, you should update your records for customers' changes of address so that goods are delivered to the correct location.

In other cases, it will be equally obvious that you do not need to update information.



## Example

An individual places a one-off order with an organisation. The organisation will probably have good reason to retain a record of the order for a certain period for accounting reasons and because of possible complaints. However, this does not mean that it has to regularly check that the customer is still living at the same address.

You do not need to update personal data if this would defeat the purpose of the processing. For example, if you hold personal data only for statistical, historical or other research reasons, updating the data might defeat that purpose.

In some cases it is reasonable to rely on the individual to tell you when their personal data has changed, such as when they change address or other contact details. It may be sensible to periodically ask individuals to update their own details, but you do not need to take extreme measures to ensure your records are up to date, unless there is a corresponding privacy risk which justifies this.

# Principle (d) – Accuracy



## Example

An organisation keeps addresses and contact details of previous customers for marketing purposes. It does not have to use data matching or tracing services to ensure its records are up to date – and it may actually be difficult to show that the processing involved in data matching or tracing for these purposes is fair, lawful and transparent.

However, if an individual informs the organisation of a new address, it should update its records. And if a mailing is returned with the message 'not at this address' marked on the envelope – or any other information comes to light which suggests the address is no longer accurate – the organisation should update its records to indicate that the address is no longer current.

# Principle (d) – Accuracy

What steps do we need to take to ensure accuracy?

Where you use your own resources to compile personal data about an individual, then you must make sure the information is correct. You should take particular care if the information could have serious implications for the individual. If, for example, you give an employee a pay increase on the basis of an annual increment and a performance bonus, then there is no excuse for getting the new salary figure wrong in your payroll records.

We recognise that it may be impractical to check the accuracy of personal data someone else provides. In order to ensure that your records are not inaccurate or misleading in this case, you must:

- accurately record the information provided;
- accurately record the source of the information;
- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information.

What is a 'reasonable step' will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for. The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate. For example, employers may need to check the precise details of job applicants' education, qualifications and work experience if it is essential for that particular role, when they would need to obtain authoritative verification.

# Principle (d) – Accuracy



## Example

An organisation recruiting a driver will want proof that the individuals they interview are entitled to drive the type of vehicle involved. The fact that an applicant states in his work history that he worked as a Father Christmas in a department store 20 years ago does not need to be checked for this particular job.

If your information source is someone you know to be reliable, or is a well-known organisation, it is usually reasonable to assume that they have given you accurate information. However, in some circumstances you need to double-check – for example if inaccurate information could have serious consequences, or if common sense suggests there may be a mistake.



## Example

A business that is closing down recommends a member of staff to another organisation. Assuming the two employers know each other, it may be reasonable for the organisation to which the recommendation is made to accept assurances about the individual's work experience at face value. However, if a particular skill or qualification is needed for the new job role, the organisation needs to make appropriate checks.



# Principle (d) – Accuracy



## Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible.



# Principle (d) – Accuracy



## Example

An individual sends an email to her mobile phone company requesting that it changes its records about her willingness to receive marketing material. The company amends its records accordingly without making any checks. However, when the customer emails again asking the company to send her bills to a new address, they carry out additional security checks before making the requested change.

Even if you originally took all reasonable steps to ensure the accuracy of the data, if you later get any new information which suggests it may be wrong or misleading, you should reconsider whether it is accurate and take steps to erase, update or correct it in light of that new information as soon as possible.

# Principle (d) – Accuracy

What should we do if an individual challenges the accuracy of their personal data?

If this happens, you should consider whether the information is accurate and, if it is not, you should delete or correct it.

Remember that individuals have the absolute right to have incorrect personal data rectified – see the [right to rectification](#) for more information.

Individuals don't have the right to erasure just because data is inaccurate. However, the accuracy principle requires you to take all reasonable steps to erase or rectify inaccurate data without delay, and it may be reasonable to erase the data in some cases. If an individual asks you to delete inaccurate data it is therefore good practice to consider this request.

# Principle (e) - Storage limitation

## At a glance

- You must not keep personal data for longer than you need it.
- You need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- You need a policy setting standard retention periods wherever possible, to comply with documentation requirements.
- You should also periodically review the data you hold, and erase or anonymise it when you no longer need it.
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data.
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

# Principle (e) - Storage limitation

What is the storage limitation principle?

Article 5(1)(e) says:

“1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')”

So, even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it.

There are close links here with the data minimisation and accuracy principles.

The UK GDPR does not set specific time limits for different types of data. This is up to you, and will depend on how long you need the data for your specified purposes.

# Principle (e) - Storage limitation

Why is storage limitation important?

Ensuring that you erase or anonymise personal data when you no longer need it will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. Apart from helping you to comply with the data minimisation and accuracy principles, this also reduces the risk that you will use such data in error – to the detriment of all concerned.

Personal data held for too long will, by definition, be unnecessary. You are unlikely to have a lawful basis for retention.

From a more practical perspective, it is inefficient to hold more personal data than you need, and there may be unnecessary costs associated with storage and security.

Remember that you must also respond to subject access requests for any personal data you hold. This may be more difficult if you are holding old data for longer than you need.

Good practice around storage limitation - with clear policies on retention periods and erasure - is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.

# Principle (e) - Storage limitation

Do we need a retention policy?

Retention policies or retention schedules list the types of record or information you hold, what you use it for, and how long you intend to keep it. They help you establish and document standard retention periods for different categories of personal data.

A retention schedule may form part of a broader 'information asset register' (IAR), or your general processing documentation.

To comply with [documentation requirements](#), you need to establish and document standard retention periods for different categories of information you hold wherever possible. It is also advisable to have a system for ensuring that your organisation keeps to these retention periods in practice, and for reviewing retention at appropriate intervals. Your policy must also be flexible enough to allow for early deletion if appropriate. For example, if you are not actually using a record, you should reconsider whether you need to retain it.

If you are a small organisation undertaking occasional low-risk processing, you may not need a documented retention policy.

However, if you don't have a retention policy (or if it doesn't cover all of the personal data you hold), you must still regularly review the data you hold, and delete or anonymise anything you no longer need.



# Principle (e) - Storage limitation

How should we set retention periods?

The UK GDPR does not dictate how long you should keep personal data. It is up to you to justify this, based on your purposes for processing. You are in the best position to judge how long you need it.

You must also be able to justify why you need to keep personal data in a form that permits identification of individuals. If you do not need to identify individuals, you should anonymise the data so that identification is no longer possible.

For example:

- You should consider your stated purposes for processing the personal data. You can keep it as long as one of those purposes still applies, but you should not keep data indefinitely 'just in case', or if there is only a small possibility that you will use it.



## **Example**

A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons for a further set time.

# Principle (e) - Storage limitation

## Example

A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

## Example

A tracing agency holds personal data about a debtor so that it can find that individual on behalf of a creditor. Once it has found the individual and reported to the creditor, there may be no need to retain the information about the debtor – the agency should remove it from their systems unless there are good reasons for keeping it. For example, if the agency has also been asked to collect the debt on behalf of the creditor.

- You should consider whether you need to keep a record of a relationship with the individual once that relationship ends. You may not need to delete all personal data when the relationship ends. You may need to keep some information so that you can confirm that the relationship existed – and that it has ended – as well as some of its details.

# Principle (e) - Storage limitation

## Example

A business may need to keep some personal data about a previous customer so that they can deal with any complaints the customer might make about the services they provided.

## Example

An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records – such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details.

## Example

A business receives a notice from a former customer requiring it to stop processing the customer's personal data for direct marketing. It is appropriate for the business to retain enough information about the former customer for it to stop including that person in future direct marketing activities.

# Principle (e) - Storage limitation

- You should consider whether you need to keep information to defend possible future legal claims. However, you could still delete information that could not possibly be relevant to such a claim. Unless there is some other reason for keeping it, personal data should be deleted when such a claim could no longer arise.

## Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

- You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If you keep personal data to comply with a requirement like this, you will not be considered to have kept the information for longer than necessary.
- You should consider any relevant industry standards or guidelines. For example, credit reference agencies keep consumer credit data for six years. Industry guidelines are a good starting point for standard retention periods and are likely to take a considered approach. However, they do not guarantee compliance. You must still be able to explain why those periods are justified, and keep them under review.

You must remember to take a proportionate approach, balancing your needs with the impact of retention on individuals' privacy. Don't forget that your retention of the data must also always be fair and lawful.

# Principle (e) - Storage limitation

When should we review our retention?

You should review whether you still need personal data at the end of any standard retention period, and erase or anonymise it unless there is a clear justification for keeping it for longer. Automated systems can flag records for review, or delete information after a pre-determined period. This is particularly useful if you hold many records of the same type.

It is also good practice to review your retention of personal data at regular intervals before this, especially if the standard retention period is lengthy or there is potential for a significant impact on individuals.

If you don't have a set retention period for the personal data, you must regularly review whether you still need it.

However, there is no firm rule about how regular these reviews must be. Your resources may be a relevant factor here, along with the privacy risk to individuals. The important thing to remember is that you must be able to justify your retention and how often you review it.

You must also review whether you still need personal data if the individual asks you to. Individuals have the absolute right to erasure of personal data that you no longer need for your specified purposes.



# Principle (e) - Storage limitation

What should we do with personal data that we no longer need?

You can either erase (delete) it, or anonymise it.

You need to remember that there is a significant difference between permanently deleting personal data, and taking it offline. If personal data is stored offline, this should reduce its availability and the risk of misuse or mistake. However, you are still processing personal data. You should only store it offline (rather than delete it) if you can still justify holding it. You must be prepared to respond to subject access requests for personal data stored offline, and you must still comply with all the other principles and rights.

The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue is to ensure you put the data beyond use. If it is appropriate to delete personal data from a live system, you should also delete it from any back-up of the information on that system.

Alternatively, you can anonymise the data so that it is no longer "in a form which permits identification of data subjects".

Personal data that has been pseudonymised – eg key-coded – will usually still permit identification. Pseudonymisation can be a useful tool for compliance with other principles such as data minimisation and security, but the storage limitation principle still applies.



# Principle (e) - Storage limitation

How long can we keep personal data for archiving, research or statistical purposes?

You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes.

Although the general rule is that you cannot hold personal data indefinitely 'just in case' it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. For example, pseudonymisation may be appropriate in some cases.

This must be your only purpose. If you justify indefinite retention on this basis, you cannot later use that data for another purpose - in particular for any decisions affecting particular individuals. This does not prevent other organisations from accessing public archives, but they must ensure their own collection and use of the personal data complies with the principles.

# Principle (e) - Storage limitation

How does this apply to data sharing?

If you share personal data with other organisations, you should agree between you what happens once you no longer need to share the data. In some cases, it may be best to return the shared data to the organisation that supplied it without keeping a copy. In other cases, all of the organisations involved should delete their copies of the personal data.



## **Example**

Personal data about the customers of Company A is shared with Company B, which is negotiating to buy Company A's business. The companies arrange for Company B to keep the information confidential, and use it only in connection with the proposed transaction. The sale does not go ahead and Company B returns the customer information to Company A without keeping a copy.

The organisations involved in an information-sharing initiative may each need to set their own retention periods, because some may have good reasons to retain personal data for longer than others. However, if you all only hold the data for the purposes of the data-sharing initiative and it is no longer needed for that initiative, then all organisations with copies of the information should delete it.

# Principle (f) – Integrity + Confidentiality (Security)

## At a glance

You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

- A key principle of the UK GDPR is that you process personal data securely by means of 'appropriate technical and organisational measures' – this is the 'security principle'.
- Doing this requires you to consider things like risk analysis, organisational policies, and physical and technical measures.
- You also have to take into account additional requirements about the security of your processing – and these also apply to data processors.
- You can consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- Where appropriate, you should look to use measures such as pseudonymisation and encryption.
- Your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- The measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- You also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.
- We have worked closely with the National Cyber Security Centre (NCSC) to develop [an approach](#) that you can use when assessing the measures that will be appropriate for you.

# Principle (f) – Integrity + Confidentiality (Security)

What does the UK GDPR say about security?

Article 5(1)(f) of the UK GDPR concerns the 'integrity and confidentiality' of personal data. It says that 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, using appropriate technical or organisational measures' ”

You can refer to this as the UK GDPR's 'security principle'. It concerns the broad concept of **information security**.

This means that you must have appropriate security in place to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

You need to consider the security principle alongside Article 32 of the UK GDPR, which provides more specifics on the security of your processing. Article 32(1) states:

# Principle (f) – Integrity + Confidentiality (Security)

What does the UK GDPR say about security?

Article 5(1)(f) of the UK GDPR concerns the 'integrity and confidentiality' of personal data. It says that 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, using appropriate technical or organisational measures' ”

You can refer to this as the UK GDPR's 'security principle'. It concerns the broad concept of **information security**.

This means that you must have appropriate security in place to prevent the personal data you hold being accidentally or deliberately compromised. You should remember that while information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

You need to consider the security principle alongside Article 32 of the UK GDPR, which provides more specifics on the security of your processing. Article 32(1) states:

“ 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' ”



# Principle (f) – Integrity + Confidentiality (Security)

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.



# Principle (f) – Integrity + Confidentiality (Security)

Why should we worry about information security?

Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – lives may even be endangered in some extreme cases.

Some examples of the harm caused by the loss or abuse of personal data include:

- identity fraud;
- fake credit card transactions;
- targeting of individuals by fraudsters, potentially made more convincing by compromised personal data;
- witnesses put at risk of physical harm or intimidation;
- offenders at risk from vigilantes;
- exposure of the addresses of service personnel, police and prison officers, and those at risk of domestic violence;
- fake applications for tax credits; and
- mortgage fraud.

Although these consequences do not always happen, you should recognise that individuals are still entitled to be protected from less serious kinds of harm, for example embarrassment or inconvenience.

Information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.

The ICO is also required to consider the technical and organisational measures you had in place when considering an administrative fine.

# Principle (f) – Integrity + Confidentiality (Security)

What do our security measures need to protect?

The security principle goes beyond the way you store or transmit information. Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);
- the data you hold is accurate and complete in relation to why you are processing it; and
- the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

These are known as 'confidentiality, integrity and availability' and under the UK GDPR, they form part of your obligations.

What level of security is required?

The UK GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.

# Principle (f) – Integrity + Confidentiality (Security)

What organisational measures do we need to consider?

Carrying out an information risk assessment is one example of an organisational measure, but you will need to take other measures as well. You should aim to build a culture of security awareness within your organisation. You should identify a person with day-to-day responsibility for information security within your organisation and make sure this person has the appropriate resources and authority to do their job effectively.



## **Example**

The Chief Executive of a medium-sized organisation asks the Director of Resources to ensure that appropriate security measures are in place, and that regular reports are made to the board.

The Resources Department takes responsibility for designing and implementing the organisation's security policy, writing procedures for staff to follow, organising staff training, checking whether security measures are actually being adhered to and investigating security incidents.

Clear accountability for security will ensure that you do not overlook these issues, and that your overall security posture does not become flawed or out of date.

# Principle (f) – Integrity + Confidentiality (Security)

Although an information security policy is an example of an appropriate organisational measure, you may not need a 'formal' policy document or an associated set of policies in specific areas. It depends on your size and the amount and nature of the personal data you process, and the way you use that data. However, having a policy does enable you to demonstrate how you are taking steps to comply with the security principle.

Whether or not you have such a policy, you still need to consider security and other related matters such as:

- co-ordination between key people in your organisation (eg the security manager will need to know about commissioning and disposing of any IT equipment);
- access to premises or equipment given to anyone outside your organisation (eg for computer maintenance) and the additional security considerations this will generate;
- business continuity arrangements that identify how you will protect and recover any personal data you hold; and
- periodic checks to ensure that your security measures remain appropriate and up to date.

# Principle (f) – Integrity + Confidentiality (Security)

What technical measures do we need to consider?

Technical measures are sometimes thought of as the protection of personal data held in computers and networks. Whilst these are of obvious importance, many security incidents can be due to the theft or loss of equipment, the abandonment of old computers or hard-copy records being lost, stolen or incorrectly disposed of. Technical measures therefore include both physical and computer or IT security.

When considering physical security, you should look at factors such as:

- the quality of doors and locks, and the protection of your premises by such means as alarms, security lighting or CCTV;
- how you control access to your premises, and how visitors are supervised;
- how you dispose of any paper and electronic waste; and
- how you keep IT equipment, particularly mobile devices, secure.

In the IT context, technical measures may sometimes be referred to as 'cybersecurity'. This is a complex technical area that is constantly evolving, with new threats and vulnerabilities always emerging. It may therefore be sensible to assume that your systems are vulnerable and take steps to protect them.

When considering cybersecurity, you should look at factors such as:

- system security – the security of your network and information systems, including those which process personal data;
- data security – the security of the data you hold within your systems, eg ensuring appropriate access controls are in place and that data is held securely;



# Principle (f) – Integrity + Confidentiality (Security)

- online security – eg the security of your website and any other online service or application that you use; and
- device security – including policies on Bring-your-own-Device (BYOD) if you offer it.

Depending on the sophistication of your systems, your usage requirements and the technical expertise of your staff, you may need to obtain specialist information security advice that goes beyond the scope of this guidance. However, it's also the case that you may not need a great deal of time and resources to secure your systems and the personal data they process.

Whatever you do, you should remember the following:

- your cybersecurity measures need to be appropriate to the size and use of your network and information systems;
- you should take into account the state of technological development, but you are also able to consider the costs of implementation;
- your security must be appropriate to your business practices. For example, if you offer staff the ability to work from home, you need to put measures in place to ensure that this does not compromise your security; and
- your measures must be appropriate to the nature of the personal data you hold and the harm that might result from any compromise.



# Principle (f) – Integrity + Confidentiality (Security)

What do we do when a processor is involved?

If one or more organisations process personal data on your behalf, then these are data processors under the UK GDPR. This can have the potential to cause security problems – as a data controller you are responsible for ensuring compliance with the UK GDPR and this includes what the processor does with the data. However, in addition to this, the UK GDPR's security requirements also apply to any processor you use.

This means that:

- you must choose a data processor that provides sufficient guarantees about its security measures;
- your written contract must stipulate that the processor takes all measures required under Article 32 – basically, the contract has to require the processor to undertake the same security measures that you would have to take if you were doing the processing yourself; and
- you should ensure that your contract includes a requirement that the processor makes available all information necessary to demonstrate compliance. This may include allowing for you to audit and inspect the processor, either yourself or an authorised third party.

At the same time, your processor can assist you in ensuring compliance with your security obligations. For example, if you lack the resource or technical expertise to implement certain measures, engaging a processor that has these resources can assist you in making sure personal data is processed securely, provided that your contractual arrangements are appropriate.

# Principle (f) – Integrity + Confidentiality (Security)

Are we required to ensure our security measures are effective?

Yes, the UK GDPR specifically requires you to have a process for regularly testing, assessing and evaluating the effectiveness of any measures you put in place. What these tests look like, and how regularly you do them, will depend on your own circumstances. However, it's important to note that the requirement in the UK GDPR concerns your measures in their entirety, therefore whatever 'scope' you choose for this testing should be appropriate to what you are doing, how you are doing it, and the data that you are processing.

Technically, you can undertake this through a number of techniques, such as vulnerability scanning and penetration testing. These are essentially 'stress tests' of your network and information systems, which are designed to reveal areas of potential risk and things that you can improve.

In some industries, you are required to undertake tests of security measures on a regular basis. The UK GDPR now makes this an obligation for all organisations. Importantly, it does not specify the type of testing, nor how regularly you should undertake it. It depends on your organisation and the personal data you are processing.

You can undertake testing internally or externally. In some cases it is recommended that both take place.

Whatever form of testing you undertake, you should document the results and make sure that you act upon any recommendations, or have a valid reason for not doing so, and implement appropriate safeguards. This is particularly important if your testing reveals potential critical flaws that could result in a personal data breach.

# Principle (f) – Integrity + Confidentiality (Security)

What about our staff?

The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process that data unless you have instructed them to do so. It is therefore vital that your staff understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice.

You should provide appropriate initial and refresher training, including:

- your responsibilities as a data controller under the UK GDPR;
- staff responsibilities for protecting personal data – including the possibility that they may commit criminal offences if they deliberately try to access or disclose these data without authority;
- the proper procedures to identify callers;
- the dangers of people trying to obtain personal data by deception (eg by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks), or by persuading your staff to alter information when they should not do so; and
- any restrictions you place on the personal use of your systems by staff (eg to avoid virus infection or spam).

Your staff training will only be effective if the individuals delivering it are themselves reliable and knowledgeable.

# Accountability Principle

## At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the UK GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must, take including:
  - adopting and implementing data protection policies;
  - taking a 'data protection by design and default' approach;
  - putting written contracts in place with organisations that process personal data on your behalf;
  - maintaining documentation of your processing activities;
  - implementing appropriate security measures;
  - recording and, where necessary, reporting personal data breaches;
  - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
  - appointing a data protection officer; and
  - adhering to relevant codes of conduct and signing up to certification schemes.

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles.

# Accountability Principle

- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

## What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are **responsible** for complying with the GDPR. Second, you must be able to **demonstrate** your compliance.

Article 5(2) of the GDPR says:

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)



# Accountability Principle

## Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

## What do we need to do?

Accountability is not a box-ticking exercise. Being **responsible** for compliance with the UK GDPR means that you need to be proactive and organised about your approach to data protection, while **demonstrating** your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the UK GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.



# Accountability Principle

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Article 24(1) of the UK GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the UK GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

# Accountability Principle

## Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The UK GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for instance, you handle large volumes of personal data, or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake ([see below for more on data protection officers](#)).

## Do we need to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

# Accountability Principle

What documentation should we maintain?

Under Article 30 of the UK GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a great way to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the UK GDPR such as making sure that the information you hold about people is accurate and secure.

As well as your record of processing activities under Article 30, you also need to document other things to show your compliance with the UK GDPR. For instance, you need to keep records of consent and any personal data breaches.

# Accountability Principle

How do we record and report personal data breaches?

You must report certain types of personal data breach to the Information Commissioner's Office (ICO), and in some circumstances, to the affected individuals as well.

Additionally, the UK GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this.

# Accountability Principle

Should we carry out data protection impact assessments (DPIAs)?

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the UK GDPR, while also acting as documented evidence of your decision-making and the steps you took.

Should we assign a data protection officer (DPO)?

Some organisations are required to appoint a DPO. A DPO's tasks include advising you about the UK GDPR, monitoring compliance and training staff.

Your DPO must report to your highest level of management, operate independently, and have adequate resources to carry out their tasks.

Even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the UK GDPR.

# What is a SAR?





# What is a SAR?

“A SAR is a request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 of the UK GDPR.” – **ICO**

Under the Subject Access provisions of the GDPR legislation an individual is entitled to **personal information** held by any organisation subject to certain parameters. This does not include any third-party information or data which can identify another individual.

A SAR helps individuals to understand how and why we are using their data and enables them to verify that it is being processed lawfully (and that it is accurate). Provision of the supplementary information within the response to the requestor, by reference to the Privacy Notice etc., helps to achieve this.

# What is personal data?

Personal data is any information relating to an identified or identifiable **living** individual.

An identifying characteristic could include a name, ID number, an image or location data. Personal data also includes expressions of opinion about the individual. Some personal data will not identify the individual by name but could still be considered the personal data of the requestor by linking it to other information held by the force. The ICO would advise that forces should treat such information as personal data even if it can only be potentially linked to a living individual. Context will be particularly relevant in such instances. Ordinarily the data must provide particular information about that individual.

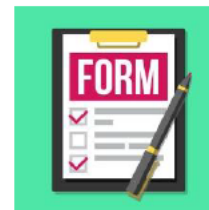


# What makes a valid SAR?

So long as the request is clear in that the individual is asking for their own personal data then it will be a valid request, whether the request is made verbally or in writing, even if or where the request cites other legislation, such as the Freedom of Information Act 2000.

However, the timescale for responding to a SAR does not begin until the information requested to verify the identity of the requestor has been received.

There is no obligation upon the individual to explain why they are making the request. Requests received via force social media channels should also be processed but an alternative response address should be sought from the applicant. There is no requirement for the request to be made in writing. However, it is advisable to encourage individuals to complete a subject access form or to apply in writing via the force website. This will ensure that the requisite information is provided by the requestor in order to assist in the handling of their request efficiently and effectively.



# Identification requirements

The Force has the right to ask individuals to provide documentary proof to verify their identity where appropriate and / or there is doubt as to the identity of the subject. The applicant should be required to send photocopies (not originals) of two official documents, at least one of which must be photographic and at least one must provide the current address. This is to ensure proof of ID and should cover address and photograph; in particular photographic ID is advised when digital images are sought. The ID documents should be checked to make sure the person who has filled in the form is the person on the ID – check the name, DOB, POB, former names etc.



# SAR's received on behalf of others

If a request is made by a third-party, it is the third-party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

## Information rights third-party consent

Someone else can make an information rights application on your behalf (to get, change or delete information the police have about you).

For them to do that, you must complete this form, sign it and give it to them. They will give it to the police or upload it online when they make the application.

I, the data subject (your name)

consent to (name of the person applying on your behalf)

being given a copy of information police hold about me, or asking for information about me to be changed or deleted

Your signature



# On behalf of a child

It is the child (or young person) who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those, such as guardians, with parental responsibility for them ('parent'). The parent can exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

In all such cases, consideration must be given to requesting the young person's birth or adoption certificate, or other evidence to show the parent has parental responsibility for him/her. However, caution must be exercised when dealing with requests where it is clear that the young person's parents are in dispute with one another, or the matter relates to an assault on the child by the parents or a sexual assault on the child etc., as the request may not be in the best interests of the young person. Where two parents (both with verified parental responsibility) have made a request, it may be appropriate to provide the child's information to both parties as they both have an equal right and vested interest. However, caution should be used to ensure neither parent receive the other parent's data as part of the disclosure, unless consent is given



# Requests received from prisoners

Where a request is received from a prison inmate, verification of ID should be undertaken by a check of Prisoner Intelligence Notification System (PINS).

ICO engagement has previously established that it is not appropriate to contact the prison to verify ID.

Due to the fact that the response is not likely to be handed directly back to the inmate without other parties accessing the documents, it is suggested that if the applicant is a serving prisoner all third-party data should be redacted, including third-party data in any statements.

# Timescales for compliance with SARs

The data to which the subject is entitled must be provided without undue delay and within one calendar month from the date of receipt. If the corresponding date falls on a weekend or public holiday, then a force will have until the next working day to respond.

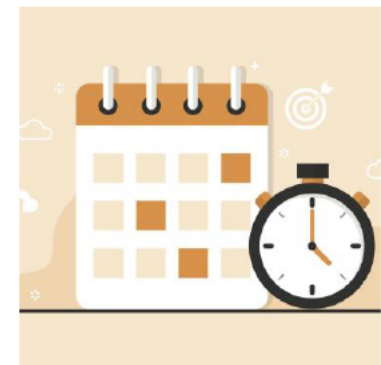
Where there is any doubt about the identity of the applicant, the clock does not start ticking until verification of the requestor's identity has been completed. If the request is for general information and processed under UK GDPR, where a large amount of information is processed about the individual and it is not clear what they are seeking, clarification may be sought as to what they specifically require – the clock can be paused until clarification received

Individuals should be informed that the clock 'has stopped' during further engagement / correspondence.



# Extension

When individuals apply for locally held information by a force, they may be asking for information such as crime reports, incident logs, statements, Professional Standards Department (PSD) files, HR files etc. This is a mixture of Crime and Non-Crime data. When a large volume of information is held and processed under UK GDPR and the request is considered 'complex' the timescales for responding may be extended by a further two months, from the date of receipt.



# Manifestly unfounded

It is not necessary to comply with a SAR if it is manifestly unfounded or excessive. The application of manifestly unfounded / excessive will require careful consideration on a case-by-case basis. Just because it is burdensome does not mean that it will be excessive.

Manifestly unfounded and excessive have not been defined in the legislation. ICO guidance states that a request may be manifestly unfounded if:

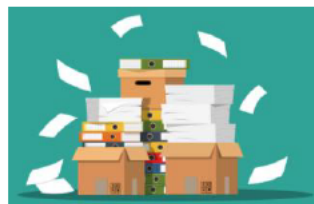
- the individual clearly has no intention to exercise their Right of Access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example
  - o the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption;
  - o the individual makes unsubstantiated accusations against the person dealing with the request or specific employees;
  - o the individual is targeting a particular employee against whom they have some personal grudge; or
  - o the individual systematically sends different requests to you as part of a campaign, e.g. once a week, with the intention of causing disruption

# Excessive

The burden will be on the Force to demonstrate that the request is manifestly excessive. The ICO guidance highlights the following factors to consider when balancing proportionality with the burden of costs in dealing with the request:

- the nature of the requested information;
- the context of the request, and the relationship between you and the individual;
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual;
- the force's available resources;
- whether the request largely repeats previous requests and a reasonable interval hasn't elapsed; or
- whether it overlaps with other requests (although if it relates to a separate set of information it is unlikely to be excessive)

A request will not be excessive just because it involves a large volume of information.



# The right to information not documents

Subject access provides a right for the requester to access their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply redacted copies of original documents but there is no obligation to do this.

If a document primarily contains non-personal data or information which is the personal data of others it is likely to be considered more appropriate to extract the relevant personal data into a summary document. And in doing so the removal of duplicate records is advised where possible e.g. when dealing with an email exchange use the last email if all the other emails are within it



# General redaction considerations

Every disclosure is very much subjective and requires consideration in context, in particular taking account of operational, investigative and third-party confidentiality considerations. Blanket exemptions should not be applied to documents. It is also necessary to take account of what information may already have previously been provided or is known to the data subject. Whatever method is to be used to formulate the disclosure; the following types of information should be considered for redaction;

## **Operational information**

- Any police operation names



# General redaction considerations

## **Third party information**

As highlighted previously the right of access is to the personal data of the individual not documents, so where appropriate the personal data may be extracted and provided within a summary document.

## **Officer / Staff Names**

If the names are already known then depending on the circumstances and context they may be left in, however in line with the data minimisation principle, it is suggested that generally officers names are removed, and collar numbers provided i.e. “PC 1111 Alexander”.

# Data held on the Police National computer (PNC)

If an individual only seeks access to information held on the Police National Computer (PNC) and is not asking for information held locally by a Force, then this will be dealt with by ACRO



# Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

[Information Commissioner's Office \(ICO\)](#)

**ico.**

Information Commissioner's Office

# Acronyms

| SAR  | Subject Access Request           |
|------|----------------------------------|
| FOI  | Freedom of Information           |
| DPA  | Data Protection Act              |
| ICO  | Information Commissioners Office |
| ACRO | Criminal Records Office          |
| ABI  | Association of British Insurers  |
| DPO  | Data Protection Officer          |
|      |                                  |
|      |                                  |



# Acronyms

| PSD    | Professional Standards Directorate      |
|--------|-----------------------------------------|
| FCC    | Force contact centre                    |
| BWV    | Body worn video                         |
| OIC/IO | Officer in charge/Investigating officer |
| OHU    | Occupational Health Unit                |
|        |                                         |
|        |                                         |
|        |                                         |
|        |                                         |



# Useful links

## ICO links;

- **Right of access** - [Right of access | ICO](#)
- **Personal data** - [What is personal information: a guide | ICO](#)
- **Dealing with a SAR** - [How to deal with a request for information: a step-by-step guide | ICO](#)

**ACRO** - [Home \(acro.police.uk\)](http://acro.police.uk)

**GMP online SAR form** - [Ask for information about yourself | Greater Manchester Police \(gmp.police.uk\)](#)

**GMP information rights** - [Your information rights | Greater Manchester Police \(gmp.police.uk\)](#)

**DPA 2018** - [Data Protection Act 2018 \(legislation.gov.uk\)](http://legislation.gov.uk)





Subject:

Date:

Attachments:



FW: Mailbox

05 September 2024 16:11:47

[image001.png](#)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Subject: RE: Mailbox

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

ACCESS

raised that we need to ensure we are adhering to equality by providing sufficient avenues to make a complaint, I have reviewed the Stat Guidance, chapter 2 Accessing the complaints system:

*All those in the police service and those overseeing it share responsibility for increasing awareness of the police complaints system and promoting access to it. They must ensure they make provisions for access to the system that reflect the needs, expectations and rights of complainants, and that those provisions do not deter members of the public from making complaints.*

Promoting access

*2.4 online – forces and local policing bodies should have clear links on the home page of their websites to information about how to make a complaint. 16 Statutory guidance on the police complaints system • social media – information about how to make a complaint should be readily available on social media accounts and pages. Forces and local policing bodies should recognise that, for some complainants, social media may be the preferred method for raising complaints, and they should take steps to manage this. Police forces are not expected to scour social media for expressions of dissatisfaction, however, where someone directs a post at the force, where they are intending to raise a complaint, and they appear to meet the definition of a complainant (see Chapter 5), police forces should ensure that there are systems in place to bring that post to the attention of the department/body responsible for the initial handling of a complaint, for logging and handling. • in police stations and custody suites – posters and leaflets about the complaints system should be displayed in public areas of police premises, including custody areas and front desks. Those in police custody must be able to make a complaint while in custody, if they wish to do so*

*2.8 Forces and local policing bodies must ensure that members of the public who wish to make a complaint can do so in a variety of ways. This should include access to paper-based forms, online forms, an email address, telephone numbers and, where practical, face-to-face meetings*  
I am satisfied we are providing all of the above apart from the email address, however, we have provided sufficient other means and thus it is accessible to all and managing reasonable adjustments.

[REDACTED]

[illegible]

103

## Comms to custody

18 September 2024 10:02:01

[2024\\_09\\_16 PSD Mailbox Bulletin 2024.jpg](#)  
[Expression of Dissatisfaction V.3.pdf](#)  
[Standards Managers .docx](#)  
[psd\\_conduct\\_referral\\_template.docx](#)  
[dsi\\_referral\\_template.docx](#)

\_\_\_\_\_

\_\_\_\_\_

DSI, adverse incident, complaint and conduct matters must not be sent to

[REDACTED]. As of yesterday the PSD have now discontinued the use of that mailbox for both the public and the force as the force moves to a system where all complaints submitted directly by members of the public must go through single online home (SOH). There has been comms work gone out to internal stakeholders, but we understand new procedures can take a little time to bed in. See also the [REDACTED] as to the change.

Any person serving with GMP who sends an e-mail to [REDACTED] will receive an auto-response directing them to the correct channel of reporting, however from PSD's monitoring of the activity in the last 24 hours we know in some transactions to the discontinued mailbox, some Custody branch staff have not followed the direction on the auto-reply as to how they must refer. That is not to be accusatory, it's just to highlight the current position and act on it to ensure that matters from custody still reach PSD i.e., we cannot afford to miss a custody referral to PSD.

The referral procedures that must be followed is set out below:

## Complaints

If custody take a complaint from a member of the public there are two options:

1. Fill out the details on single online home on behalf of the member of the public.
2. Fill out a 711 'Expression of dissatisfaction' form [as attached] and send it to

**[This e-mail address must not be given to the public** - it is for internal use only and does not receive mail from external domains].

## Conduct,



[REDACTED]

**DSI and adverse incidents**

[REDACTED]

[REDACTED]

Kind regards

[REDACTED] Detective Chief Superintendent | Professional Standards Directorate

[REDACTED]

GSC: Official (unless otherwise stated)



Policing, Crime, Criminal Justice and Fire  
Greater Manchester Combined Authority

Via e-mail

**Professional Standards Directorate**  
Greater Manchester Police  
Unit A  
Central Park  
Northampton Road  
Manchester  
M40 5BP

12<sup>th</sup> September 2024



### **Changes to making public complaints to Greater Manchester Police**

I'm emailing, on behalf of Greater Manchester Police's Professional Standards Directorate, to inform you of a change to the way the force receives complaints – to ensure all complaints are assessed and progressed in a consistent, efficient, and effective manner.

From 7am on Tuesday 17 September 2024, complaints to GMP should be submitted via the accessible online form at [Make a complaint about the police | Greater Manchester Police \(gmp.police.uk\)](https://gmp.police.uk). Those with accessibility requirements can continue to make complaints via 101, at their local police station, or in writing. Those with hearing or speech impairments can use our textphone service – 18001 101.

Whilst the online form has been an option for some time, this removes the option to submit complaints via e-mail. An automatic reply has been added to the mailbox redirecting senders to the online form.

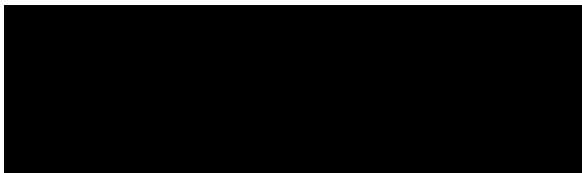
Complaints can continue to be made via third parties including the Local Policing Body – Greater Manchester Combined Authority (GMCA), and The Independent Office for Police Conduct (IOPC).

A new email address (REDACTED) has been created to accommodate correspondence from GMCA, the IOPC and other professional organisations. An automatic reply has also been added to this mailbox to redirect anyone who wishes to make a new complaint or follow up an existing complaint to the online form.

In the event you are contacted directly from a person wishing to express dissatisfaction or follow up an existing complaint, please direct them to the online portal so as to ensure a consistent level of service.

Thank you for your continued support as we strive to build public trust and confidence.

Yours sincerely,



Detective Chief Inspector



**From:** [REDACTED]  
**Subject:** Single Online Home - Please read  
**Date:** 21 August 2024 15:19:00

---

All

[REDACTED]  
[REDACTED]  
[REDACTED]

The purpose of this email is primarily aimed at the assessment unit staff as it effects them directly but equally for those of you who work duty cover it will also have an impact on you to a degree.

For the rest of you receiving this email it is an update which will alter the way in which the PSD receive public complaints and as it is so significant it is vital you are informed in advance to avoid any confusion.

On Tuesday 17<sup>th</sup> September the PSD will take over the responsibility of Single Online Home (SOH) from the Force Contact Crime Operations (FCCO) Branch.

The reason being, GMP is one of very few forces who's PSD does not have responsibility and ownership of their SOH function and are therefore reliant upon the FCCO to send through those complaints which need to be assessed by PSD, this means on occasion we are not sighted on potentially critical complaints and this is a risk for PSD and the force.

There are some recent examples of where we have missed complaints which have become critical and we could have reduced the criticality of those complaints had we been sighted on them earlier.

[REDACTED] has last week and some of this week has completed some testing of SOH to understand the true demand this will place upon us as it goes without saying this means we will be triaging and assessing additional complaints from the point we go live. [REDACTED] will however feedback that the triaging of complaints received via SOH is far more straight forward than some of those emails you will be familiar with seeing land in the existing mailbox and as such this gives us a far better starting position when receiving an initial complaint.

Please note the large majority of the complaints that enter via SOH that we don't already know about are not serious and are in the main are suitable for handling outside schedule 3 and or other than by investigation, however this is why auto population will be crucial to ensure we are able to record them as efficiently as possible given the increased demand. We are yet to learn exactly what portion of the complaints that exist within SOH also exist within Centurion having been assessed by PSD ie they are duplicates.

Another significant change is that as of the same date the discipline and complaints mailbox will no longer exist and we will adopt a private industry approach to the public wishing to make a public complaint. Instead the public will be sign posted towards SOH to raise their complaint. This will force complainants to complete all relevant criteria before submitting and removes the

ease for a complainant to fire in multiple emails to an inbox. There is also a maximum word count so it prevents complainants from providing unnecessarily long text which take considerable time to unpick to identify and record allegations this will therefore save us some time.

There will be a new mailbox which will enable external partners to email in such as our colleagues from IOPC, GMCA, CC office, however this will be set up with an intelligent auto response which advises a complainant that complaints must be submitted via SOH and we will adopt strict rules for the handling of this mailbox to ensure it does not become a replacement for the existing mailbox, your support with regards to this will be vital.

We will also have a new conduct mailbox which will enable referrals from districts and branches which relate to conduct matters or DSI's similar to the way we receive these types of referrals now, again we will maintain strict rules to ensure this is not misused either internally or externally.

I appreciate this change is radical and is totally different to what many of you have been used to for many years. This decision has been carefully thought out and a large degree of planning has and continues to be invested to ensuring we get this right. We have taken aspects of other forces and other private industry models to devise this innovative approach and whilst that which I have set out above appears straight forward I know this will take some time to bed in and will no doubt require tweaking as we go along. This is where I require all of your help in ensuring this lands successfully and feeding back where you identify issues or have ideas which could improve things.

The way in which we currently receive complaints is placing unprecedented demand upon us and the above is designed in such a way to enable a fair and transparent public complaint process whilst balancing this with ensuring the system is not abused and we can provide as efficient service as possible.

Over the next couple of weeks there will be further engagement with our key stakeholders such as IOPC, GMCA, CC office and FCCO to ensure that by go live date we get ourselves in the strongest position to ensure the above transition is smooth as it can be.

If you have any concerns about anything set out above please do come and speak with me.

Thank you in advance for your support with the above plan.

Regards

[REDACTED]

[REDACTED] | Detective Chief Inspector | Professional Standards Directorate |  
Greater Manchester Police

[REDACTED]  
[REDACTED]

GSC: Official (unless otherwise stated)

## Screenshot - GMP Intranet Guidance on Handling Complaints

### Who can complain?

- The person directly affected
- A person who has been adversely affected
- A witness to the conduct
- A third party acting on behalf of one of the aforementioned (with written third party authority) for example – parent/ support worker/partner/solicitor/local counsellor.

### How can someone complain?

How to complain about the police | Greater Manchester Police

- Via the IOPC – completing a standardised web based form
- Via GMP website - completing a standardised form, also know as "Single Online Home"
- In writing to PSD
- Via 101
- In person at a station – the officer will need to complete an expression of dissatisfaction form and submit to

**NOT TO BE SHARED WITH THE PUBLIC - INTERNAL USE ONLY.**