# GENERAL NOTES FOR USING THE TEMPLATE INTERNAL INDIVIDUALs’ RIGHTS POLICY & PROCEDURE

This Individuals’ Rights Policy and Procedure is intended to be an internal document setting out how a request for any of the following rights under the GDPR which will come into effect on 25 May 2018:

* + 1. A right to have personal data rectified
    2. A right to erasure i.e. a right to be forgotten
    3. A right to object to the processing of their personal data
    4. A right to restriction of processing
    5. A right to data portability

This policy and procedure does not cover the handling of subject access requests. This is dealt with in a separate template policy called “Internal Subject Access Request Policy”.

This Individuals’ Rights Policy and Procedure is intended to be given to employees, volunteers and other staff members in order for them to recognise a request for any of the matters listed above and for employees to know what to do with any request once it is received.

In order for this Individuals’ Rights Policy and Procedure to be effective, it must **accurately reflect** the way in which your organisation operates.

There are a number of areas in square brackets which require your input and amendment. Once you have determined what to include in the areas in square brackets you should amend the area in square brackets and remove the square brackets.

This front sheet should be deleted before the Privacy Policy is provided to any individual and all areas in red need to be considered by you and amended appropriately.

# INTERNAL INDIVIDUALs’ RIGHTS POLICY & PROCEDURE

## This policy and procedure deals with the handling of requests by individuals in relation to their personal data

*NB. This policy and procedure does not cover the handling of subject access requests. If you are dealing with a subject access request see [NAME OF ORGANISATION]’S Internal Subject Access Request Policy [INSERT LINK].*

1. Introduction
   1. [NAME OF ORGANISATION] holds personal data about a number of individuals including; job applicants, employees, [customers], [members], suppliers, business contacts and other individuals for a variety of purposes.
   2. Under data protection law, individuals have rights in relation to the processing of their personal data:
      1. A right to have personal data rectified (see section 4);
      2. A right to erasure i.e. a right to be forgotten (see section 5);
      3. A right to object to the processing of their personal data (see section 6);
      4. A right to restriction of processing (see section 7); and
      5. A right to data portability (see section 8);
   3. Determining when these rights can be exercised by individuals, when specific exemptions apply and what [NAME OF ORGANISATION]’s compliance obligations are in relation to these rights under data protection law, are complicated.
   4. This policy sets out the procedure for dealing with requests received by [NAME OF ORGANISATION] from individuals to exercise the rights listed in 1.2 above.
   5. This policy provides guidance for staff members on how such requests should be dealt with, and is intended for internal use. [It is not to be made routinely available to third parties.]
   6. This policy is aimed primarily at those members of staff who are authorised to handle such requests. For other staff members, it provides guidance on:
      1. How to decide on the nature of the request (i.e. which right it relates to); and
      2. What to do if a request is received.
   7. A failure to comply with a request in relation to the rights listed in 1.2 above, could result in a breach of data protection law by [NAME OF ORGANISATION], as such a failure by staff members to comply with this policy may lead to disciplinary action, which could result in dismissal, depending on the particular circumstances of the case (see section 11).

**Handling requests**

1. Identifying a request
   1. A request from an individual in relation to any of the rights outlined in 1.2 above does not need to expressly refer to personal data, any Data Protection Act, the General Data Protection Regulation or other relevant data protection law.
   2. A request can be made verbally, in person or over the telephone, or in writing through any media e.g. email, letter, fax or social media.
   3. All requests in relation to any of the rights outlined in 1.2 above (in whatever form they are received e.g. telephone, e-mail, fax, social media etc.) should be immediately directed to an authorised member of staff, which include the following:
      1. [Data Protection Officer or equivalent],
      2. [Head of legal]
      3. [Head of HR]
      4. [Other]
   4. There are limited timescales within which [NAME OF ORGANISATION] must respond to a request (see section 3 below) and any delay could result in our failing to meet those timescales, which could lead to a breach of data protection laws [,enforcement action by the Information Commissioner and/or legal action by the affected individual].
   5. We must take reasonable steps to verify the identity of the individual making the request at the outset.
2. The timescale for responding to a request
   1. A valid request should be responded to without undue delay and at least within 1 calendar month of the request being received by [NAME OF ORGANISATION].
   2. The timescale referred to in 3.1 above will begin to run once a request is received by [NAME OF ORGANISAITON]. As such, it is imperative that if a staff member received a request in relation to the rights set out in section 1.2, that it is passed immediately to an authorised member of staff (as set out in 2.3 above).
   3. In exceptional circumstances, it may be possible to extend this period by a further 2 calendar months, providing 3 calendar months in total to respond.
   4. Such an extension will only be applicable where the request is complex of voluminous, such as, where a request relates to, or overlaps with, a number of the different rights set out in section 1.2 above. Only an authorised member of staff (as outlined in 2.3 above) should determine whether an extension can be applied. If an extension is applied, the individual must be notified of that fact and the reasons for the extension without delay.

# The rights of individuals

1. The right to have personal data rectified (rectification)
   1. An individual has the right to have personal data that is processed by [NAME OF ORGANISATION] rectified if it is inaccurate or incomplete.
   2. All requests for rectification should be immediately directed to an authorised member of staff, which include the following:
      1. [Data Protection Officer or equivalent],
      2. [Head of legal]
      3. [Head of HR]
      4. [Other]
   3. Upon receipt of the request for rectification by the authorised member of staff, the processing of the personal data in question should immediately be restricted (in accordance with section 7) while the accuracy of the personal data is determined.
   4. The personal data the individual claims is inaccurate or incomplete should then be located and reviewed to determine its accuracy.
   5. The right of rectification only applies to objective and factual data, not to subjective statements (which, by definition, cannot be factually wrong). For example, in the context of a staff appraisal a subjective evaluation made by a line manager in the staff appraisal report cannot be rectified, whereas the name, the grade or any other factual data can. [In certain circumstances, it may be appropriate to consider whether a statement from the individual should be included with the disputed personal data ].
   6. If it is determined that the personal data being processed by [NAME OF ORGANISATION] is inaccurate, the inaccuracy should be rectified and the individual notified.
   7. This request for rectification must be fulfilled, and the individual notified, in accordance with the time limits set out in section 3 above.
   8. Consideration should be given to all of the locations where that the inaccurate or incomplete personal data in question may be processed, for example inaccurate personal data may be processed in a hard copy personnel file and on [NAME OF ORGANISATION]’s website. Care should be taken to ensure the inaccurate personal data is rectified in all locations.
   9. If it is determined that the personal data being processed is inaccurate or incomplete, and [NAME OF ORGANISATION] has disclosed that personal data to 3rd parties e.g. other business or organisations. We are under an obligation to inform those 3rd parties that the individual’s personal data requires rectification, unless this proves impossible or involves disproportionate effort. If the individual requests it, we may also be under an obligation to inform them about the 3rd parties to whom we have disclosed their personal information.
   10. In the event that the accuracy of the personal data is disputed i.e. [NAME OF ORGANISATION] maintains that the personal data we are processing in relation to the individual is accurate, the individual should be informed (in accordance with the time limits set out in section 3 above) of:
       1. the fact that [NAME OF ORGANISATION] considers that the personal data being processed in relation to the individual is accurate;
       2. the basis for this determination; and
       3. the fact that the request for rectification will not be fulfilled.

Any refusal should meet the requirements set out in section 10 below.

1. A right to erasure i.e. a right to be forgotten (erasure)
   1. An individual has the right to have their personal information erased and no longer processed.
   2. This right is available to an individual only if one of the following specific circumstances applies:
      1. The personal data being processed by [NAME OF ORGANISATION] is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
      2. [NAME OF ORGANISATION] is processing the personal data on the legal basis of consent, the individual withdraws that consent, and there is no other legal basis upon which we can rely to process the individual’s personal data;
      3. The individual objects to processing and [NAME OF ORGANISATION] has no legitimate grounds for the processing;
      4. The individual objects to the processing of their personal data for direct marketing purposes;
      5. [NAME OF ORGANISATION] has processed the individual’s personal data unlawfully;
      6. [NAME OF ORGANISATION] is under a legal obligation to erase the personal data [(e.g. when a criminal conviction becomes spent)];
      7. The personal data relates to a child (i.e. under 16 years of age) and it has been collected in relation to the offer of information society services.
   3. All requests for erasure should be immediately directed to an authorised members of staff, which include the following:
      1. [Data Protection Officer or equivalent],
      2. [Head of legal]
      3. [Head of HR]
      4. [Other]
   4. Upon receipt of the request for erasure by the authorised member of staff, the processing of the personal data in question should immediately be restricted (in accordance with section 7).
   5. In the event that one of the specific circumstances set out in 5.2 above apply, consideration should be given to whether one of the following exemptions apply in the circumstances:
      1. [NAME OF ORGANISATION] needs to process the individual’s personal data in order to comply with a legal obligation;
      2. It is necessary to proses the individual’s personal data for the establishment exercise or defence of a legal claim, either relating to [NAME OF ORGANISATION] or a 3rd party;
      3. [NAME OF ORGANISATION] needs to process the individual’s personal data for reasons of public interest in the area of public health (e.g. the provision of health or social care, ensuring the high standards of health and social care or protecting against serious cross-border threats to health);
      4. Processing is necessary for exercising the right of freedom of expression and information;
      5. Processing is necessary for archiving purposes in the public interest, scientific or historical purposes or statistical purposes if erasing the individual’s personal data will seriously impair or make it impossible to achieve the objectives of that processing.
   6. Where one of the specific circumstances set out in 5.2 above applies, and none of the exemptions set out in 5.4 above apply, the individual has the right to have their personal data erased and no longer processed by [NAME OF ORGANISATION].
   7. [NAME OF ORGANISATION] should inform the individual that their request for erasure has been fulfilled.
   8. In the event that [NAME OF ORGANISATION] has made the personal data of the individual public e.g. published the information online, we must take all reasonable steps, including technical measures (taking account available technology and the cost involved) to inform all 3rd parties who are processing the individual’s personal data to erase any links to, or copies of, or replications of the personal data.
   9. This request for erasure must be fulfilled, and the individual notified, in accordance with the time limits set out in section 3 above.
   10. In the event that one of the specific circumstances set out in 5.2 above does not apply, or an exception to the right of erasure as set out in 5.5 above applies, the individual should be informed (in accordance with the timescales set out in section 3 above) that:
       1. None of the specific circumstances necessary to exercise the right of erasure apply, and therefore the individual cannot exercise their right of erasure; or
       2. That one of the specific circumstances necessary to exercise the right of erasure does apply, however [NAME OF ORGANISATION] considers that an exemption applies in the circumstances, which prevents the individual’s personal data from being erased. The individual should be informed of the applicable exemption and the basis upon which [NAME OF ORGANISATION] considers it applies.

Any refusal should meet the requirements set out in section 10 below.

1. A right to object to the processing of their personal data (objection)

**Direct marketing**

* 1. An individual has an absolute right to object to the processing of their personal data for the purposes of direct marketing (including profiling).
  2. Where the individual has objected to the processing of their personal data for direct marketing purposes [NAME OF ORGANISATION] must stop processing their personal data for such purposes.
  3. All objections to processing for the purposes of direct marketing should be immediately directed to [the Head of Marketing/Other].
  4. The objection to processing for direct marketing purposes must be honored in accordance with the time scales set out in section 3 above.
  5. The individual’s details must be removed from any marketing databases but must be retained on [NAME OF ORGANISATION]’s Suppression List to ensure that their details are not re-entered onto any marketing database in the future.

**Scientific or historical research or statistical purposes**

* 1. An individual has the right to object to the processing of their personal data for scientific or historical research or statistical purposes.
  2. Where the individual has objected to the processing of their personal data for these purposes [NAME OF ORGANISATION] must stop processing their personal data for such purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest.
  3. All objections in relation to processing for the purposes of scientific or historical research or statistical purposes should be immediately directed to [Data Protection Officer/Compliance Officer/Other].
  4. If applicable the objection to processing for scientific or historical research or statistical purposes must be honored in accordance with the time scales set out in section 3 above.

**Processing for other purposes (including profiling)**

* 1. An individual has the right to object to the processing of their personal data for purposes other than direct marketing and scientific or historical research or statistical purposes if one of the following applies:
     1. The individual’s personal data is being processed on the basis that processing is necessary for the performance of a task carried out in the public interest, [or in the exercise of [NAME OF ORGANISATION]’s official authority]; or
     2. The individual’s personal data is being processed on the basis that processing is necessary for the purposes of the legitimate interests pursued by [NAME OF ORGANISATION] or a 3rd party.
  2. All objections to processing should be immediately directed to an authorised member of staff, which include the following:
     1. [Data Protection Officer or equivalent],
     2. [Head of legal]
     3. [Head of HR]
     4. [Other]
  3. If either of the grounds set out in 6.10 above applies, [NAME OF ORGANISATION] must stop processing the individual’s personal data unless:
     1. [NAME OF ORGANISATION] can demonstrate a compelling legitimate ground for processing the individual’s personal data, which overrides their rights; or
     2. [NAME OF ORGANISATION] can demonstrate that processing is necessary for the establishment, exercise or defence of legal claims.
  4. Where one of the grounds set out in section 6.10 above applies and [NAME OF ORGANISATION] cannot demonstrate one of the grounds set out in 6.12 above we must stop processing their personal data.
  5. The objection to processing must be honored in accordance with the time scales set out in section 3 above.
  6. In the event that one of the specific circumstances set out in 6.10 above does not apply, or [NAME OF ORGANISATION] considers it can demonstrate one of the circumstances set out in 6.12 above, the individual should be informed (in accordance with the timescales set out in section 3 above) that:
     1. The specific circumstances necessary to exercise the right of objection do not apply, and therefore the individual cannot exercise their right of objection in this instance; or
     2. The specific circumstances necessary to exercise the right of objection do apply, however [NAME OF ORGANISATION] considers that we have a compelling legitimate ground for processing the individual’s personal data that overrides their right to object in this instance. The basis of this assertion should be set out; or
     3. The specific circumstances necessary to exercise the right of objection do apply, however [NAME OF ORGANISATION] considers that we can demonstrate that processing is necessary for the establishment, exercise or defence of a legal claim which override the individual’s right to object in this instance[, if appropriate broad details of the nature of this claim should be set out] .

Any refusal should meet the requirements set out in section 10 below.

1. The right of restriction of processing (restriction)
   1. An individual has the right to request that [NAME OF ORGANISATION] restricts (i.e. blocks or suppresses) the processing of their personal data.
   2. This right is available to an individual where one of the following applies:
      1. The accuracy of the personal data is contested by the individual (see section 4 above) (in such circumstances [NAME OF ORGANISATION] should restrict the processing until the accuracy of the personal data is verified).
      2. The processing is unlawful and the individual opposes erasure and requests restriction instead.
      3. Where an individual has objected to the processing where it was necessary for the performance of a task in the public interest or on the basis of legitimate interests (see section 6 above), and we are considering whether [NAME OF ORGANISATION]’s legitimate grounds override those of the individual.
      4. [NAME OF ORGANISATION] no longer needs the personal data for the purposes of processing, but the individual requires the personal data to establish, exercise or defend a legal claim.
   3. All requests for restriction should be immediately directed to an authorised member of staff, which include the following:
      1. [Data Protection Officer or equivalent],
      2. [Head of legal]
      3. [Head of HR]
      4. [Other]
   4. Where one of the circumstances set out in 7.2 applies, processing of the individual’s personal data by [NAME OF ORGANISATION] must be restricted (i.e. blocked or suppressed) unless one of the following exemptions apply:
      1. The individual has consented to the processing of the restricted personal data;
      2. Processing is necessary for the establishment, exercise or defence of legal claims;
      3. Processing is necessary for the protection of the rights of another individual; or
      4. Processing is necessary for reasons of important public interest.
   5. In the event that one of the specific circumstances set out in 7.2 above does not apply, or [NAME OF ORGANISATION] considers one of the exemptions set out in 7.4 applies, the individual should be informed that their request for restriction will not be actioned and the reasons why (in accordance with the timescales set out in section 3 above). Any refusal should meet the requirements set out in section 10 below.
   6. Where one of the circumstances set out in 7.2 applies and none of the exemptions in section 7.4 applies, processing of the individual’s personal data by [NAME OF ORGANISATION] must be restricted. In order to ensure that the processing of the personal data of an individual is restricted in accordance with the individual’s request one or more of the following may be necessary:
      1. Temporarily moving the relevant personal data to another processing system;
      2. Making the relevant personal data unavailable to [staff and other] users of [NAME OF ORGANISAITON]’s systems;
      3. Temporarily removing published data from [NAME OF ORGANISATION]’s website [and any associated websites].
      4. Ensuring (by technical means) that the relevant personal data is not subject to further processing and cannot be changed.
      5. Ensuring that the fact that the processing of the relevant personal data is restricted is clearly marked on the system.
   7. The restriction on processing must take place in accordance with the time scales set out in section 3 above.
   8. Where the processing of personal data is restricted, and [NAME OF ORGANISATION] has disclosed that personal data to 3rd parties e.g. other business or organisations. We are under an obligation to inform those 3rd parties that the processing of the relevant personal data is restricted, unless this proves impossible or involves disproportionate effort.
   9. If [NAME OF ORGANISATION] determines that the restriction on the processing of the relevant personal data should be lifted (for example if any dispute about the accuracy of the personal data is resolved). We must inform the individual that we have decided to lift the restriction on processing their personal data.
2. The right to data portability (data portability)
   1. An individual has the right to request that their personal data is provided to them in a structured, commonly used and machine-readable format to enable them to obtain and reuse their personal data for their own purposes across different services.
   2. This right is available to an individual only if all of the following apply:
      1. The personal data has been provided to [NAME OF ORGANISATION] by the individual;
      2. The processing is based on the individual’s consent or for the performance of a contract; and
      3. The processing is carried out by automated means (i.e. electronically).
   3. All requests for data portability should be immediately directed to an authorised member of staff, which include the following:
      1. [Data Protection Officer or equivalent],
      2. [Head of legal]
      3. [Head of HR]
      4. [Other]
   4. Where the right to data portability applies [NAME OF ORGANISATION] must provide the individual’s personal data in a structured, commonly used and machine-readable form in accordance with the time scales set out in section 3 above.
   5. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.
   6. An individual also has the right to request that their personal data is transmitted directly to another organisation. [NAME OF ORGANISATION] must comply with such a request if this is technically feasible in accordance with the time scales set out in section 3 above, however we are not required to adopt or maintain processing systems that are technically compatible with other organisations in order to comply with such a request.
   7. Where an individual requests data portability in relation to personal data that concerns more than one individual [NAME OF ORGANISATION] must consider whether providing the information would adversely affect the rights of any other individual.
   8. Where [NAME OF ORGANISATION] determines that a request for data portability will not be actioned, for example because the requirements of section 8.2 above do not apply, or providing the personal data would adversely affect the rights of others, we must inform the individual of this fact and explain the reasons why their request will not be actioned in accordance with the time scales set out in section 3 above. Any refusal should meet the requirements set out in section 10 below.
3. Charging a fee
   1. In the majority of cases a response to, and compliance with, any of the individual rights set out in 1.2 above where applicable, will be free of charge.
   2. If however, a request from an individual is considered to be manifestly unfounded or excessive in nature (for example because a request is repetitive), it is possible to:
      1. Charge a reasonable fee taking into account the administrative costs of taking the action requested; or
      2. Refuse to act on the request.
   3. If a request to exercise any of the individual rights set out in 1.2 above is suspected of being manifestly unfounded or excessive in nature it should be referred to the [Data Protection Officer or other] without delay.
   4. Only the [Data Protection Officer or other] has the authority to determine:
      1. Whether the request is in fact manifestly unfounded or excessive in nature, if so:
         1. Whether a fee should be charged in relation to taking the action requested, and the level of that fee (the fee should be based on the administrative cost of taking the action requested); or
         2. Whether to refuse to act on the request.
   5. If it is determined that a fee should be charged, the individual should be notified, in writing, of that fact, the level of the fee, and the reason for requesting the fee, without delay. The time limit as set out in section 3 above will not begin to run until the fee is received by [NAME OF ORGANISATION].
4. Refusing a request
   1. If it is determined that a request in relation to any of the rights set out in section 1.2 above will be refused, the data subject should be notified, in writing, of that fact and the reasons for the refusal to act on the request and informed of their right to complain to the supervisory authority and to a judicial remedy, without delay and in accordance in accordance with the time scales set out in section 3 above.
5. [Review of response to a request]
   1. An individual will be informed of their right to review the response they receive to a request in relation to any of the rights set out in section 1.2 above. They will be provided with details of how to request a review of the response.
   2. The review will be undertaken by the [Data Protection Officer or other] .]
6. Disciplinary action
   1. A failure to comply with this guidance may be a disciplinary offence, which could result in summary dismissal.
7. Review of this policy
   1. This procedure will be reviewed [specify period] by the [Data Protection Officer or other].
   2. Any questions regarding this procedure should be addressed to the [Data Protection Officer or other] [insert contact details].