YOUR GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR)

1 What is this Regulation all about?

1.1 The General Data Protection Regulation 2016 (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. The Government have set out in a Data Protection Act 2018 some provisions for how the GDPR will apply in the UK. The requirements of GDPR are enforceable by the Information Commissioner's Office from the 25 May 2018. The Regulation governs what we do with personal data and what rights members of the public have concerning their own personal data.

2 What is Personal Data?

2.1 The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

2.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

2.3 The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

2.4 Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

2.5 The information includes facts, opinions and plans about the person as well as audio, video or CCTV images by which that person can be identified.

2.6 Certain categories of personal information are classified under GDPRt as special categories of sensitive personal data. This form of personal data relates to a person's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; or criminal convictions or proceedings. Under the Regulation the processing of sensitive personal data can only be carried out under strict conditions.

2.7 One change is that the GDPR includes genetic data and some biometric data in the definition. Another is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data.

2.8 Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, the Council must identify both a lawful basis and a separate condition for processing special category data. These do not have to be linked.

2.8 There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Bill will introduce additional conditions and safeguards. The Council must determine a condition for processing special category data before we carry out any processing under the GDPR, and this should be documented. More detailed guidance on the special category conditions and how they differ from existing Data Protection Act Schedule 3 conditions will follow as the Data Protection Act 2018 is finalised.

3 The Data Protection Principles

3.1 Under the GDPR, the data protection principles set out the main responsibilities for organisations.

3.2 These state that data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
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;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
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;
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; and
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.

3.3 The Council as a data controller is responsible for, and able to demonstrate, compliance with the principles

4 Why do we keep personal information?

4.1 We provide a range of services to people and communities and to do this we need to collect a certain amount of personal information. This allows us to maintain a record of the services people have requested and ensure that we deliver effective and efficient services to them.

5 How is my personal data protected?

5.1 We regard the lawful and correct treatment of personal information as vital. We have put controls in place to ensure that personal data is processed lawfully and kept secure. Further details of this are set out in our Data Protection Policy.

6 What are my Rights under the Act?

6.1 You have the right to:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

7 How do I make a Subject Access Request?

7.1 If you would like more information about what we hold about you personally, you can do so verbally , in writing or by completing a Subject Access Request Form, which you will find towards the end of these notes. Please print the form off, then complete and return it to the address given at the end of the form. The request can be made to any part of the Council including by social media and does not have to be to a specific person or contact point.

7.2 Someone else (e.g. parent, legal guardian or Solicitor) can make a request on your behalf so long as you provide your written consent, which can be sent in with the request.

7.3 The majority of requests will be responded to without a charge. Where the request is manifestly unfounded or excessive we may charge a "reasonable fee" for the administrative costs of complying with the request. We can also charge a reasonable fee if an individual requests further copies of their data following a request. We must base the fee on the administrative costs of providing further copies.

8 How do we process a request?

8.1 We will act on the subject access request without undue delay and at the latest within one month of receipt. The time limit will be calculated from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

8.2 If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.

8.3 If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

8.4 This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

8.5 We can extend the time to respond by a further two months if the request is complex or if we have received a number of requests from an individual. We must let the individual know within one month of receiving their request and explain why the extension is necessary.

8.6 However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- it is manifestly unfounded or excessive;
- an exemption applies; or
- we are requesting proof of identity before considering the request.

8.7 If we have doubts about the identity of the person making the request we can ask for more information. We will only request information that is necessary to confirm who they are. The key to this is proportionality. Please see link below with recommended proof of identity.

https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist#proof-of-identity-checklist-for-individuals

8.8 We will let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when we receive the additional information.

8.9 If we process a large amount of information about an individual we can ask for more information to clarify their request. We should only ask for information that we reasonably need to find the personal data covered by the request.

8.10 We will let the individual know as soon as possible that we need more information from them before responding to their request. The period for responding to the request begins when we receive the additional information. However, if an individual refuses to provide any additional information, we will endeavour to comply with their request by making reasonable searches for the information covered by the request.

9 Requests for information about children?

9.1 Even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian. So it is the child 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 with parental responsibility for them.

9.2 Before responding to a subject access request for information held about a child, We should consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we should usually respond directly to the child. We may, however, allow the parent to 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.

9.3 What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, we should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have

10 What happens if we give incorrect or incomplete information?

10.1 Under GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

10.2 We have to provide you with all of the personal information that we hold about you as an individual. This includes information held both on computer and in manual or accessible records.

10.3 In addition to providing your personal information, we will also provide:
Other information

10.4 In addition to a copy of their personal data, we also have to provide individuals with the following information:

- the purposes of your processing;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- the retention period for storing the personal data or, where this is not possible, the criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

10.5 More information about how we process your personal data is shown in our Privacy Notice.

https://www.northwarks.gov.uk/privacy

11 What is the right to rectification?

11.1 Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

11.2 If we do not agree that the information is inaccurate, you have the right to record your disagreement on the record itself. In addition, you can appeal to the Information Commissioner or the Courts. These bodies have the power to order us to correct information which is wrong.

11.3 If you believe that you have not been given all the information asked for, you can appeal to us through our Complaints and Compliments Procedure, or after that to the Information Commissioner.

12 What is the right to erasure?

12.1 Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

13 When does the right to erasure apply?

13.1 Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);

- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

14 How does the right to erasure apply to data collected from children?

14.1 There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the GDPR.

14.2 Therefore, if you process data collected from children, you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

15 Do we have to tell other organisations about the erasure of personal data?

15.1 The GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

15.2 If you have disclosed the personal data to others, you must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, you must also inform the individuals about these recipients.

15.3 The GDPR defines a recipient as a natural or legal person, public authority, agency or other body to which the personal data are disclosed. The definition includes controllers, processors and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

15.4 Where personal data has been made public in an online environment reasonable steps should be taken to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable you should take into account available technology and the cost of implementation.

16 When does the right to erasure not apply?

16.1 The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.
- The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:
- if the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

17 Can we refuse to comply with a request for other reasons?

17.1 You can refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

17.2 If you consider that a request is manifestly unfounded or excessive you can:
- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

17.3 In either case you will need to justify your decision.

17.4 You should base the reasonable fee on the administrative costs of complying with the request. If you decide to charge a fee you should contact the individual promptly and inform them. You do not need to comply with the request until you have received the fee.

18 What is the right to restrict processing?

18.1 Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

18.2 Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

19 When does the right to restrict processing apply?

19.1 Individuals have the right to request you restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 21(1), and you are considering whether your legitimate grounds override those of the individual.
- Although this is distinct from the right to rectification and the right to object, there are close links between those rights and the right to restrict processing:
- if an individual has challenged the accuracy of their data and asked for you to rectify it (Article 16), they also have a right to request you restrict processing while you consider their rectification request; or
- if an individual exercises their right to object under Article 21(1), they also have a right to request you restrict processing while you consider their objection request.

19.2 Therefore, as a matter of good practice you should automatically restrict the processing whilst you are considering its accuracy or the legitimate grounds for processing the personal data in question.

20 What is the right to data portability?

20.1 The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

21 When does the right apply?

21.1 The right to data portability only applies when:

- your lawful basis for processing this information is consent **or** for the performance of a contract; and
- you are carrying out the processing by automated means (ie excluding paper files).

22 What does the right apply to?

22.1 Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to you.

23 What does 'provided to a controller' mean?

23.1 Sometimes the personal data an individual has provided to you will be easy to identify (eg their mailing address, username, age). However, the meaning of data 'provided to' you is not limited to this. It is also personal data resulting from observation of an individual's activities (eg where using a device or service).

23.1 This may include:

- history of website usage or search activities;
- traffic and location data; or
- 'raw' data processed by connected objects such as smart meters and wearable devices.
- What is the right to object?
- Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask you to stop processing their personal data.
- The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing.

24 When does the right to object apply?

24.1 Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

24.2 Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in you; or
- your legitimate interests (or those of a third party).

24.3 In these circumstances the right to object is not absolute.

24.4 If you are processing data for scientific or historical research, or statistical purposes, the right to object is more limited.

24.5 These various grounds are discussed further below:-

Direct marketing

- An individual can ask you to stop processing their personal data for direct marketing at any time. This includes any profiling of data that is related to direct marketing.

- This is an absolute right and there are no exemptions or grounds for you to refuse. Therefore, when you receive an objection to processing for direct marketing, you must stop processing the individual's data for this purpose.

- However, this does not automatically mean that you need to erase the individual's personal data, and in most cases it will be preferable to suppress their details. Suppression involves retaining just enough information about them to ensure that their preference not to receive direct marketing is respected in future.

Processing based upon public task or legitimate interests

An individual can also object where you are relying on one of the following lawful bases:
- 'public task' (for the performance of a task carried out in the public interest),
- 'public task' (for the exercise of official authority vested in you), or
- legitimate interests.

24.5 An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

24.6 In these circumstances this is not an absolute right, and you can continue processing if:

- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal

25 **<u>Do we need to tell individuals about the right to object?</u>**

25.1 The GDPR is clear that you must inform individuals of their right to object at the latest at the time of your first communication with them where:

- you process personal data for direct marketing purposes, or
- your lawful basis for processing is:
- public task (for the performance of a task carried out in the public interest),
- public task (for the exercise of official authority vested in you), or
- legitimate interests.

25.2 If one of these conditions applies, you should explicitly bring the right to object to the individual's attention. You should present this information clearly and separately from any other information.

25.3 If you are processing personal data for research or statistical purposes you should include information about the right to object (along with information about the other rights of the individual) in your privacy notice.

26 Do we always need to erase personal data to comply with an objection?

26.1 Where you have received an objection to the processing of personal data and you have no grounds to refuse, you need to stop processing the data.

26.2 This may mean that you need to erase personal data as the definition of processing under the GDPR is broad, and includes storing data. However, as noted above, this will not always be the most appropriate action to take.

26.3 Erasure may not be appropriate if you process the data for other purposes as you need to retain the data for those purposes. For example, when an individual objects to the processing of their data for direct marketing, you can place their details onto a suppression list to ensure that you continue to comply with their objection. However, you need to ensure that the data is clearly marked so that it is not processed for purposes the individual has objected to.

26.4 The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

26.5 The GDPR applies to all automated individual decision-making and profiling.

26.6 Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

26.7 You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

26.7 You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

27 Rights of Data Subjects

27.1 So far as the rights outlined above are concerned, you can contact the Council by telephone, in person or via email and through our website. Please contact us if you have any concerns about the processing of your personal data.

27.2 In all cases, we must respond to a request within 1 calendar month of receiving it. If the request is not considered justified, we must give reasons. If we do not reply in time or you believe we have not complied with data protection requirements, you can apply to the Court for an order requiring compliance.

27.3 If you have suffered damage or distress as a result of the contravention of any of the requirements of the Act, by us, then you may be entitled to compensation. The Court will only support such a claim if you can show that we had not taken reasonable care to ensure we complied with the relevant requirement of the Act. Compensation may also be payable if you can satisfy the Court that you have suffered damage as the result of our use of inaccurate data.

28 **Complaints to the Information Commissioner**

28.1 You can complain to the Information Commissioner if you consider that we have breached any of the requirements of the General Data Protection Regulation and the, Data Protection Bill. These include a breach of any of the data protection principles, processing data without having notified the Commissioner, a failure to respond to any written notices, processing data without consent (where consent is necessary) or refusing to provide you with the personal information you have requested.

28.2 At your request, the Commissioner will carry out an assessment of the Council's processing to establish whether or not we are doing so in compliance with the Act. Should the Commissioner find we are not, then we will be issued with a notice requiring us to take steps to ensure compliance.

28.3 However, before involving the Information Commissioner, you should contact us and try to resolve the problem directly with us through our Complaints and Compliments Procedure (please see paragraph 11.4 below). If after doing this you are still not satisfied with the outcome, you should then get in touch with the Commissioner. His contact details are as follows:-

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Website: www.informationcommissioner.gov.uk
Telephone: 01625-545745
Fax: 01625-524510
E-mail: mail@ico.gsi.gov.uk

11.4 Contact details for the Complaints and Compliments Procedure are as follows:-

Phone: 01827 719238
Fax: 01827 719225 (For the attention of Policy Support)
E-Mail: complaintsandcompliments@northwarks.gov.uk
Letter or in person: Policy Support
North Warwickshire Borough Council
The Council House
South Street
Atherstone
North Warwickshire
CV9 1DE

APPENDIX A

NORTH WARWICKSHIRE BOROUGH COUNCIL

GENERAL DATA PROTECTION REGULATION (GDPR)

SUBJECT ACCESS REQUEST FORM

The General Data Protection Regulation (GDPR) gives individuals who are the subject of personal data ("data subjects") a general right of access to the personal data which are held about them. Personal data may be held electronically on computerised systems or in manual records.

If we have doubts about the identity of the person making the request we can ask for more information. We will only request information that is necessary to confirm who they are. The key to this is proportionality.

Data Subject's Details

We need your personal details to find the personal data that we hold about you. Your details will be held solely for the purpose of processing your subject access request and will not be passed to any other organisation. We will keep this form on file for one year after we reply to your request. We may transfer some of the information you give on this form to a computerised database to help us monitor and improve our performance. After one year we will destroy this form and delete identifying details from our database.

SECTION 1 - PROOF OF IDENTIFICATION

1. Are you the data subject? (Please tick appropriate box)

Yes ☐ Go to Section 1(a) No ☐ Go to Section 1(b)

1(a)

Please provide 2 **original** proofs of your identity (see below). For recommended proof of identity see link below.

https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist#proof-of-identity-checklist-for-individuals

Please state below what evidence you have enclosed:

Current car insurance certificate ☐ Current Passport ☐

Current UK Driving Licence ☐ Recent Utility Bill ☐

Current Bank Statement ☐ Current Council Tax Bill ☐

Other (please state)

1(b)

Are you acting on behalf of the data subject with their written or other legal authority?

Yes ☐ No ☐

If yes, please state your relationship with the data subject - e.g. - parent, legal, guardian, or solicitor.

Please enclose proof that you are legally authorised to obtain this information. The proof could be a letter of authority, letters or official forms addressed to you on behalf of the data subject. Photocopies cannot be accepted. Once entitlement has been established we will take a copy of the documents you have supplied to us and will return the original to you. We reserve the right to request further proof of authority if necessary.

Please state below what proof of authority you have enclosed:

Letter of authority ☐ Correspondence ☐

Official Forms ☐ Other (please state)

SECTION 2 - DATA SUBJECTS DETAILS
2 (a) - Details of the data subject

Surname: Forename(s):

Previous/ Alternative names:

Date of birth:

Current address:

House/Flat number & street:

Town/City:

County:

Post Code:

Telephone Number:

Please provide details of any previous addresses you feel may be of assistance to this request, or if you have lived at the above address for less than 2 years.

IF YOU ARE THE DATA SUBJECT PLEASE CONTINUE TO SECTION 3 2 (b) - Details of person requesting the information (if not the data subject)

Surname: Forename(s):

Name of Solicitor(s) (if applicable):

House/Flat number & street:

Town/City:

County:

Post Code:

Telephone Number:

Email address:

Would you like the information to be sent to you or the data subject? Me: □ Data subject: □

SECTION 3 - LOCATING YOUR RECORDS

In order for us to be able to locate the information you are seeking quickly and efficiently, we would ask that you complete the appropriate section(s) below.

Department (if known):

Section (if known):

Approx. dates of contact. From: **To:**

Name of Officer(s) (if known):

Any other information, which may be of help:

SECTION 4 - DECLARATION

Please read the following declaration carefully and then sign and date it. Please note that any attempt to mislead may result in prosecution.

I, ... certify that the information provided on this application is true. I understand that it is necessary for the Council to confirm my/the data subject's identity and that it may be necessary for the Council to request more details from me in order to be able to locate the correct information.

Signature:..... Date:

CHECKLIST

Please ensure you have completed the form and tick the boxes below:

Have you completed all appropriate sections? □

Have you signed and dated the form? □

Have you enclosed the appropriate proofs of identity/authority? □

Have you enclosed a stamped addressed envelope for the return of documents? □

Please return the completed form to:

The Data Protection Officer
Policy Support
North Warwickshire Borough Council
The Council House
South Street
Atherstone
North Warwickshire
CV9 1DE

Whilst we have to respond to your request for information within 28 days, please note that this time period does not begin until all of the above information has been received along with any other information we have requested.

FOR OFFICIAL USE ONLY

Date Received		**Request Number**	
Identity Checked by		**Date Acknowledged**	
Date ID Returned		**Date Response Sent**	