

HAMBLETON

DISTRICT COUNCIL

Data Protection Rights Policy

a place to

grow

Contents

Introduction and scope	3
Right of Access (subject access requests)	4
Rights to erasure, rectification and restriction	7
Right to be informed of and object to the use of automated decision making technology	9
Right to data portability	10
Access to information by third parties about deceased individuals	11
Accepting requests by third parties on behalf of the data subject	12
Data protection complaints	13
Appendix 1 - Standard costs to be used in the calculation of fees for subject access requests under the General Data Protection Regulation (GPDR) and Data Protection Act (PDA) 2018.....	14
Appendix 2 - Data protection rights extension process	15
Appendix 3 - Information governance appeals notice	16

Version: 1.0

Publication date: 3.10.19

Policy review date: 3.10.20



Introduction and scope

In May 2018 the UK's existing data protection framework was replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. As part of Hambleton District Council's compliance with this new legislative framework it has introduced a new information governance policy framework.

The Data Protection Rights Policy details how the council will comply with an individual's request to exercise their data protection rights, including the right of access, and how the council will deal with complaints and/or concerns relating to Data Protection. The policy is concerned with, in particular, the first data protection Principle:

Article 5(1)(a) Personal data should be processed lawfully, fairly, and in a transparent manner in relation to the data subject

Who does this policy apply to?

The Information Governance Strategy and corresponding policies apply to all council officers, any authorised agents working on behalf of the council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

What does this policy apply to?

The Information Governance Strategy and corresponding policies apply to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper
- information or data stored electronically, including scanned images
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- speech, voice recordings and verbal communications, including voicemail
- published web content, for example intranet and internet
- photographs and other digital images.



What is a Data Protection Right?

Chapter III of the GDPR provides data subjects with the following rights in relation to their personal data which a data controller processes:

- right to be informed ¹
- 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.

Whilst these rights are enshrined in legislation they are not absolute rights and could be subject to exemptions where required.

Right of access (Subject Access Requests)

Data Protection Information Requests, known as Subject Access Requests (SAR), apply only to the personal information of the data subject - that is the person who the data is about. Only the Data Subject, someone legitimately acting on their behalf, a legally appointed advocate of the Data Subject, or a third party who has the explicit consent of the Data Subject should be permitted to access this data.

Receiving a Request

Any officer, elected member, or contractor of the council could receive a request for personal data that is held by, or on behalf of, the council from an applicant at any time.

The DPA 2018 does not require subject access requests to be made in writing. However, applicants will be encouraged to complete the 'Subject Access Request Form' where possible to ensure the council understands the request and can more easily locate the requested information.

Requests that are received orally will be written down by the receiving officer and confirmed with the applicant by the receiving officer to ensure the council understands the applicant's request.

¹ The right to be informed is not addressed in this policy but is instead included in the council's 'Personal Privacy Policy' in relation to the publication of Privacy Notices.



All requests for personal information must be passed to the Information Governance Team. Each request received by the council will be acknowledged with the applicant within five working days by the receiving officer, a directorate representative, or the Information Governance Team. The Information Governance Team will log the request, provide a reference number and forward the request onto the responsible officer(s) to process.

The council must be satisfied as to the applicant's identity. If the Information Governance Team is not certain of the applicant's identity from existing council records or involvement with the applicant, they may ask that applicant produce:

- valid photo ID (driver's licence, passport etc)
- proof of address (utility bill, council tax letter etc)
- or sufficient information for the council to be satisfied of the applicant's identity.

A list of accepted Identification Documents will be maintained and published on the council's website. This list will be based on the Cabinet Office's recommended list of recognised identification documents.

Fees

Generally, no fee may be charged for processing a subject access request. However, where a request is considered to be 'Excessive' or 'Manifestly Unreasonable' (as defined by Article 5 of the GDPR) or where the requested information has already been supplied, under subject access, to the applicant then council may refuse a request outright or request a reasonable administrative fee.

SAR charges should be made in accordance with the subject access charging structure (Appendix 1).

Timescales

A request only becomes valid once the council is satisfied it has sufficient detail to respond to the request. Once a request is considered to be valid then the council has one calendar month to respond to the request. In most cases, for consistency, the council will interpret one calendar month to be 30 Calendar Days.

The council may apply a discretionary extension of up to two further calendar months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either complexity of the case or volume of the information. If the council wishes to apply an extension they will inform the applicant of the extension within the first thirty days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing heavy workloads. The Data Protection Officer will approve and keep a record of all time extensions. A standard threshold, for applying an extension, will be maintained by the Data Protection Officer (Appendix 2).



Searching for Information

When locating information across council filing systems, databases, and archives (electronic and manual) officers should take care to search name variations, initials, and nicknames. Officers should make a record of what search terms they have used and what systems were searched. The Data Protection Officer will provide council officers with guidance as to how to search for information and how to keep records of such searches.

Exemptions and Third Party Information

There are a range of exemptions, in the Data Protection Act, which can be applied to some or all of the information being requested. A data subject's right to their own data is very strong and the council will only apply exemptions when absolutely necessary.

Third Party data, that is data about a person other than the data subject, should also be withheld from the disclosure unless:

- the third party individual has given consent to disclosure
- they are incapable of giving consent or
- there is a reasonable expectation of disclosure (i.e the third party is a council officer or other professional working with the data subject).

The Data Protection Officer will approve and keep a record of all exemptions applied to personal data disclosed under Subject Access.

Responding to Requests

Subject access requests must be answered within the timeframes stipulated above.

Each directorate is responsible for responding to their own SARs. If the request is a cross-directorate request then the Information Governance Team will coordinate and send the response.

Whilst the council's default position will be to transmit the requested information electronically by secure means, the council is obliged to send responses in the format preferred by the applicant. Every effort will be made to comply with this requirement. If an applicant requests the information in a specific format the council is not obliged to comply unless it is reasonable to do so. Where copy documents are requested there is no requirement to send a copy of the document to the applicant. In some cases it may be easier to extract the information from the document or to provide a digest.

Officers should take care to ensure redactions are permanent and cannot be reversed. The Data Protection Officer will offer guidance to council officers as to how to secure redactions effectively and efficiently.

Officers should also take care to transmit the requested personal data by secure means:

- **Post:** 1st class recorded or special courier
- **Electronic Transmission:** Egress Email or Secure Access Portal



Rights to erasure, rectification and restriction

As well as having the Right of Access to their personal data, Data Subjects may wish to exercise their rights to request that their personal data is erased, rectified, or restricted to one specific purpose.

It is the responsibility of the Data Protection Officer, with the assistance of the relevant service area, to consider and respond to such requests.

Timescales

A request only becomes valid once the council is satisfied it has sufficient detail to respond to the request. Once a request is considered to be valid then the council has one calendar month to respond to the request. In most cases, for consistency, the council will interpret one calendar month to be 30 Calendar Days.

The council may apply a discretionary extension of up to two further calendar months to comply with the request if the request would take a considerable amount of time to action due to either complexity of the case or volume of the information. If the council wishes to apply an extension they will inform the applicant of the extension within the first thirty days of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing heavy workloads. The Data Protection Officer will approve and keep a record of all time extensions. A standard threshold, for applying an extension, will be maintained by the Data Protection Officer (Appendix 2).

Considering requests for Data Erasure

When considering a request for personal data to be erased from council systems the following considerations must be addressed:

- Whether the council requires the information for a lawful and specified purpose or purposes, (including audit, archival, and research purposes).
- Whether the information was collected based on the consent of the Data Subject.
- Whether another legislative direction compels the council to retain or destroy the personal data.
- Whether the personal data is required by the council to establish, exercise, or defend legal claims of the council, or another individual.
- Whether erasing the data would jeopardise a record of decisions made by the council.

When rejecting a request for data erasure the council will, if it is appropriate to do so, explain the reasons for not complying with the applicant's request. The council's response must outline its lawful basis for processing the personal data and the retention period, or alternatively the criteria used to determine a retention period. The council will also contemplate whether, if erasing the data is not appropriate, rectifying or restricting the data would be more appropriate.

When upholding a request for data erasure the council will ensure that all council systems, including archived records and electronic databases, will be cleansed. The council will inform the data subject when it expects this will be done and will provide the data subject with an assurance certificate stating the data has been erased.



The Data Protection Officer will maintain a log of erasure requests and whether the request was upheld or rejected. If the request was upheld, the Data Protection Officer will take care to ensure that their log, and any corresponding record, does not include the information requested to be erased.

Considering requests for Data Rectification

When considering a request for personal data to be rectified the following considerations must be addressed:

- Whether the information held on council systems is recorded as a fact, professional opinion, or statement made by a third party.
- Whether editing the data would jeopardise a record of decisions made by the council.
- Whether the Data Subject's claims that the information is incorrect can be corroborated by other sources or professionals.
- Whether editing the data could lead to fraudulent activities.

When rejecting a request for data rectification the council will, if it is appropriate to do so, explain the reasons for not complying with the applicant's request. The council will also contemplate whether it would be appropriate to attach the applicant's request to the contested information so that future readers understand that the applicant contests the accuracy of the data.

When upholding a request for data rectification the council will ensure that all council systems, including archived records and electronic databases, will be updated. The council will inform the data subject when it expects this will be done and will provide the data subject with an assurance certificate stating the data has been rectified. In some cases it may be more appropriate to annotate the record to reflect that the information is incorrect but that decisions have already been made based on the incorrect data.

The Data Protection Officer will maintain a log of rectification requests and whether the request was upheld or rejected.

Considering requests for Data Restriction

As well as requesting that data be either erased or rectified, a Data Subject may ask the council to restrict their processing activities to limited purposes.

A request for restriction will be considered to be valid if the council:

- is verifying the accuracy of the data or the lawfulness of processing upon the Data Subject's request
- does not have a lawful basis for processing the data but the data subject has asked that the council does not delete the data
- no longer requires the personal data other than for the establishment, exercising, or defence of legal claims.



Processing restrictions are not permanent and may be suspended if the council has either verified the accuracy of the data, verified the processing of the data, or a new lawful processing activity is identified. The council will inform the data subject that the processing restriction has been suspended as soon as possible.

The Data Protection Officer will maintain a log of restriction requests and whether the request was upheld or rejected.

Right to be informed of and object to the use of automated decision making technology

For some processes the council may wish to utilise Automated Decision Making technology. If this is the case then the council must, in most cases, inform Data Subjects that the technology is in use and how the Data Subject is able to object to the use of the technology on their personal data if applicable.

Definition and Scope of Automated Decision Making Technology

The Information Commissioner's Office defines Automated Decision Making as using automated algorithmic technology to make predictions or decisions about an individual based on data about their personality, behaviour, interests, or habits.

This policy does not apply to automated analysis processing where aggregated data is being used for research, to generate statistics, or to direct council policy.

The policy also does not apply to processing where automated technology has been used for a calculation but there has been human review of the calculation prior to a decision being made i.e. an assessment tool.

Informing Data Subjects

When the council does operate automated decision making technology it must inform data subjects that their personal data is, or may be, subject to the technology and decisions may be made about them as the result of the processing.

Data Subjects will be informed through the utilisation of service level Privacy Notices. ²

² The right to be informed is not addressed in this policy but is instead included in the council's 'Personal Privacy Policy' in relation to the publication of Privacy Notices.



Handling Rights to Object

The GDPR stipulates that there are two types of objection to Automated Decision Making. These are outright objections and partial objections.

Outright Objections: A Data Subject can insist that their Personal Data is not subject to Automated Decision Making if:

- the council's lawful basis for processing is in the public interest or the legitimate interests of the council,
- the personal data is being processed for the purpose of direct marketing,
- the personal data is being processed for the purpose of scientific or historical research solely about that individual.

Partial Objections: A Data Subject can insist that, if a decision is being made about them using automated means, a human being reviews that decision. This does not apply if:

- the automated decision making is required to enter in to a contract with the data subject
- UK law provides the council with a legal obligation to utilise Automated Decision Making Technology.

Objections to Automated Decision Making Technology must be overseen by the Data Protection Officer but it is the responsibility of the service area responsible for the technology to ensure the rights of the data subject are upheld when making automated decisions about the data subject. The Data Protection Officer will maintain a log of such requests,

Safeguards when using Automated Decision Making Technology

The council's 'Personal Privacy Policy' will outline what measures will be implemented in order to safeguard the rights and freedoms of the data subject when using Automated Decision Making Technology.

Right to data portability

As well as the right of access to their personal data, data subjects can also request that the council provides them, or another controller of their choice, with certain data in a machine readable format. This is known as the right to Data Portability.

Data Portability will only apply if the processing was based on the consent of the Data subject or based on contractual obligations. Data Portability will also only apply to data processed by automated means.

The Data Protection Officer will maintain a log of such requests and will work with IT to ensure that requests are processed within one calendar month.



Access to information by third parties about deceased individuals

From time to time the council may receive requests for information about individuals who are deceased. The requests usually originate from family members of the deceased.

Verifying Right of Access

If the council receives such a request it must decide if the requesting applicant has a right of access to any information about the individual. Whilst data about deceased individuals is not covered by the provisions of Data Protection legislation, the council is bound by a Duty of Confidentiality. This means that the council is not permitted to disclose information, about a deceased individual, to any person other than a personal representative of the estate.

The council must see proof that an applicant is the personal representative of an estate before disclosing any information. The proof could be a 'Grant of Probate', if the deceased left a will, or a 'Letter of Administration', if the deceased died intestate.

In most cases the council cannot disclose information to the deceased's next of kin, close family members, or individuals who have held lasting of power of attorney for the deceased, without seeing the above documentation.

Considerations

Although in usual circumstances an individual who possesses documentation, proving that they are the personal representative of deceased individual's estate, would be permitted to receive information related to the deceased - this is not always the case.

In deciding if an applicant has a right of access to information the council must consider if:

- the deceased had expressly asked the council, or another individual, to keep certain information confidential
- disclosure could prejudice the prevention and/or detection of crime
- disclosure would prejudice the confidentiality of any other individual.

Managing and Responding to Requests

As information about a deceased person is not within scope of Data Protection legislation then the council must consider releasing the information under the Freedom of Information Act 2000.

However, unlike with usual Freedom of Information requests, the Information Governance Team will be responsible for responding to requests for information about the deceased. This is due to the complexities of establishing the right of access to information. The Information Governance Team will work with the service area, and sometimes Legal Services, in deciding whether to uphold or reject a request for information.



The Information Governance Team will respond to requests within 20 Working Days as is stipulated by the Freedom of Information Act 2000. Complaints about the way requests, for information relating to a deceased person, have been processed will be covered by the council’s Information Governance appeals process (Appendix 3).

Accepting requests by third parties on behalf of the data subject

Where a Data Protection request has been received by an individual, who is acting on behalf of the Data Subject, then the council must establish the applicant’s right to exercise a data protection request.

The following table expresses what evidence must be examined before a request from a third party will be accepted:

Applicant Type	Evidence Required
On behalf of: Child Under 12 Years Old (or older child lacking mental capacity)	Demonstrable evidence that individual has parental responsibility for that child
On behalf of: Child Over 12	Child may be asked to consent or agree to disclose data to applicant in certain circumstances
On behalf of: an Adult	Official paperwork listing individual as legal guardian of the data subject
Solicitor or Agent acting on Data Subject’s behalf	A form of authority addressed specifically to the council and signed by the data subject or their legal representative. In some circumstances the council may also request explicit consent from the data subject.
Other individual acting on Data Subject’s behalf	The Data Subject may be asked to consent or agree to disclose data to an individual in certain circumstances.

Each data protection request will be decided on a case by case basis and will take in to account any exceptional factors.

When refusing a data protection request, due to no right of access being established, officers must highlight why a request has been refused and what the applicant can do to persuade the council to re-examine their request.



Data protection complaints

Unlike with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004, the GDPR and DPA 2018 do not require the council to have a statutory internal review process. However, it is considered to be best practice to have a complaints procedure in place if a Data Subject:

- believes that exemptions have been applied incorrectly or information is missing from a response to a Subject Access Request,
- believes that other Data Protection Requests have not been handled appropriately or have not taken in to consideration all factors,
- believes that the council is processing their personal data unlawfully, unfairly, or in a manner not deemed to be secure.

The council will maintain and publish an Information Governance Appeals Document so that applicants understand the process (Appendix 3). The appeals document must be attached to all responses to Data Protection rights.

The Data Protection Officer will be responsible for considering and answering such complaints. This will be in conjunction with the council's corporate complaints process. The Data Protection Officer will maintain a procedure document outlining when a complaint should be considered by the Data Protection Internal Review process and when a complaint should be considered under the corporate complaints process.

Data Protection internal reviews will be conducted and responded to within 30 Calendar Days.

If an applicant is not satisfied with the outcome of an internal review they may raise a concern with the ICO. The Information Governance Team, on the instruction of the Data Protection Officer, will act as the point of contact for the ICO in respect of concerns raised.

Appendix 1

Standard costs to be used in the calculation of fees for subject access requests under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018

Staff time ³	£25 per hour	
Printing and Photocopying Costs (per Sheet)	A4 (b/w) - 2p A3 (b/w) - 4p A0 (b/w) - £2	A4 (colour) - 10p A3 (colour) - 20p A0 (colour) - £10
Postage Costs	1 st class at cost or original estimate, whichever is lesser	
Other items such as relevant translation	At cost or original estimate, whichever is lesser	

Charging regime:

All charges will be calculated at time of request. The applicant will be advised of any charge and all payment must be settled prior to work commencing.

Only applicable where a request is considered to be 'Excessive' or 'Manifestly Unreasonable' or where copies of information, already provided under Subject Access, have been requested	
Staff time required	Charge (£) (+VAT where applicable) ⁴
Less than half an hour	Disbursement costs only
At least half an hour, but less than one full hour	£12.50 + disbursements
One full hour	£25 + disbursements*
* A further £25 will be charged for each additional full hour required to identify the information requested (with a pro rata'd calculation for part hours)	

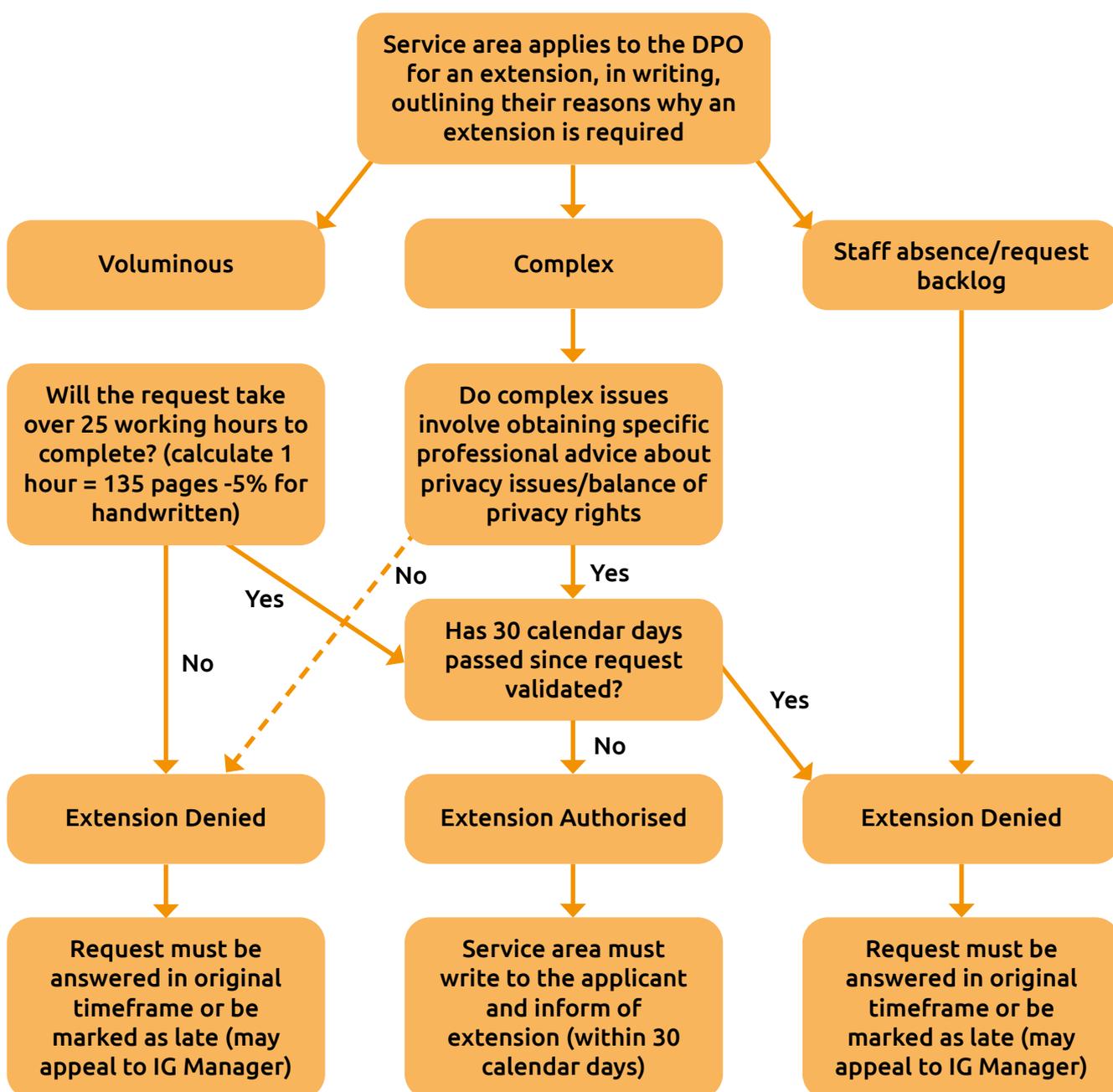
³ Activities taken into account when calculating staff time are locating, retrieving and extracting the information.

⁴ VAT will be applied in addition to charges outlined should the information requested be available to the applicant from another source other than NYCC.

Appendix 2

Data protection rights extension process

Each extension will be awarded on a case by case basis but the following diagram will be used as a standard.



Appendix 3

Information governance appeals notice

This document outlines the appeals process that services users can exercise if unhappy with the way in which a request for information has been handled. This document covers requests made under the Freedom of Information Act 2000, Environmental Information Regulations 2004, and Data Protection legislation.

Appeals regarding Freedom of Information (FOI) and Environmental Information Regulations (EIR) Requests

If you are dissatisfied in the way in which Hambleton District Council has responded to your request for information under the FOI Act or EIR then you may request that the Council conducts a statutory Internal Review. You may wish to request such a review if you:

- are dissatisfied with the way in which your request has been handled
- do not agree with an exemption that has been applied to the information you have requested
- believe that not all of the information has been provided to you.

Upon receipt the Information Governance Manager will appoint an officer to handle your complaint. Where possible the appointed officer will not have had any involvement in your original request and will have more seniority than the original responding officer. The reviewing officer will then examine your original request and the response that was sent to you and decide whether the Council responded to your request appropriately according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn decisions to withhold information.

The Council will conduct FOI and EIR Internal Reviews **within 20 Working Days**. If you are dissatisfied with the response to an Internal Review you may appeal to the Information Commissioner's Office (see overleaf).

Appeals regarding Subject Access Requests (SAR) and other Data Protection requests or concerns

If you are dissatisfied in the way in which Hambleton District Council has responded to your Subject Access Request or other Data Protection request/concern then you may request that the Council conducts an Internal Review. Unlike with the FOI/EIR process this is not a statutory requirement but is instead a stage that the Council has chosen to adopt. You may wish to request such a review if you:

- are dissatisfied with the way in which your request has been handled
- do not agree with an exemption that has been applied to the information you have requested
- believe that not all of the information has been provided to you.

Upon receipt the Information Governance Manager will appoint an officer to handle your complaint. Where possible the appointed officer will not have had any involvement in your original request and will have more seniority than the original responding officer. The reviewing officer will then examine your original request and the response that was sent to you and decide whether the Council responded to your request appropriately according to legislative requirements. The reviewing officer will also decide whether to uphold or overturn decisions to withhold information.



The Council will conduct Data Protection Internal Reviews **within 30 Calendar Days**. If you are dissatisfied with the response to an Internal Review you may appeal to the Information Commissioner's Office (see overleaf).

How to Request an Internal Review

To request that the Council requests an Internal Review you should contact the Information Governance Manager on the below contact details:

Information Governance Manager
Hambleton District Council
Stone Cross
Northallerton
North Yorkshire
DL6 2UU

Email: infogov.HambletonDC@veritau.co.uk

Telephone: 01609 532526

When requesting an Internal Review you should supply the following information:

- Your name (so that we can identify you and your request)
- Your contact details (so that we can contact you with our response)
- Request reference number (this should have been provided to you when the Council responded to your original request)
- Reasons why you are dissatisfied with the response to your request

The Information Governance Office will acknowledge your request for an internal review within 5 working days and advise you of timescales for responding.

Please be aware that Internal Reviews will not usually be conducted if 2 Calendar Months have passed since your request was responded to.

After the Council has considered your appeal

If, following the completion of an internal review, you still remain dissatisfied with the way in which the Council has handled your request then you may appeal to the Information Commissioner's Office (ICO). The ICO is the UK's Freedom of Information and Data Protection Regulator.



You can do this by contacting:

First Contact Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow Cheshire
SK9 5AF

Email: casework@ico.gov.uk

Phone: 0303 123 1113

If you are dissatisfied with the ICO's response to your complaint then you may be able to take your complaint to the information tribunal. The ICO will give you details about this when they issue their decision notice.



a place to
grow

HAMBLETON
DISTRICT COUNCIL

Civic Centre, Stone Cross, Rotary Way, Northallerton, North Yorkshire DL6 2UU
01609 779977

hambleton.gov.uk



This information is available in alternative formats and languages