Information Security Document

Corporate Subject Access Request Procedures

Version 11.0

Version History			
Version	**Date**	**Detail**	**Author**
2.0	30/09/2004	Published	Stuart Estrella-Pinto
3.0	10/02/2012	Reviewed and Approved by Information Governance Group. Version 2.0 taken as core and totally reworked and due to timescale agreed by email..	Jenny Barnes
4.0	27/03/2013	Reviewed by Information Governance Group	Lucie Collard
5.0	11/08/2014	Reviewed by Information Governance Group	Liz Wild
6.0	14/09/2015	Reviewed by Information Governance group	Liz Wild
7.0	10/07/2017	Reviewed by Information Governance Group. Updates to ICO guidance, exemptions re-ordered and SAR contacts added.	Janet Gardom
8.0	21/05/2018	Updated to take into account ICO audit actions, Data Protection Act 2018 and GDPR.	Sinead Roberts
9.0	11/06/2018	Reviewed by Information Governance Group.	Sinead Roberts
10.0	18/12/2018	Reviewed by Information Implementation Group. Group fed back identification requirements overly stringent.	Sinead Roberts
10.0	04/03/2019	Reviewed by Information Governance Group. Rules relaxed if subjects do not have original documents.	Sinead Roberts
11.0	06/08/2019	Reviewed by Information Governance Group.	Sinead Roberts

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.3	Protection of records
A.18.1.4	Privacy and Protection of personally identifiable information

CONTENTS

Data Protection Act 2018
Subject Access Requests

Introduction

In delivering services to the public, it is necessary for the Council to process a significant amount of personal data relating to individuals. The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (the Act) give individuals a number of rights, including a right to obtain a copy of their personal data as well as other supplementary information. This right of access, is often referred to as a right of "subject access". It helps individuals understand how and why you are using their data, and checks you are doing it lawfully.

In addition to rights in relation to accessing their data the Data Protection Act 2018 and GDPR give individuals a number of additional rights including the right to rectification (correction of inaccurate data), the right to erasure (sometimes referred to as the right to be forgotten), the right to restrict processing and the right to object to the processing of their data. Some of these rights are qualified rights, which means there are some exceptions to them; further information in relation to these rights is contained in the Council's Personal Rights procedure which can be found at www.derbyshire.gov.uk/gdpr

Requests for information in accordance with the Data Protection Act 2018 differ from requests for information under the Freedom of Information Act 2000 by virtue of the fact that the information identifies the requester and is about them personally.

Under the Act the Council has a legal obligation to provide a copy of the data to the requester without undue delay and at the latest within 1 month of receipt. If the request is particularly complex, or repeated, in some cases it is possible to extend the period by a further 2 months. In addition to receiving their personal data, individuals also have a right to know why you are processing their personal data, the categories of data you are processing, who you share this information with, how long you keep their information for, where it originated from, how it is stored, who they can complain to if they are not happy with the way their information has been handled and how their information is safeguarded. Some of this information is likely to be included in the Council's privacy notices at www.derbyshire.gov.uk/privacynotices and the Council's retention schedules at www.derbyshire.gov.uk/retentionschedules

This procedure details the way in which the Council should process a SAR request; a step by step procedure is followed by more detailed guidance notes to assist officers responsible for processing requests of this kind. Some departments may produce supplementary guidance on how information is stored and retrieved within their offices and these should be used in conjunction with this procedure.

The Information Commissioner's Office also produces helpful guidance which is regularly updated and will assist in ensuring that the Council is following best practice. Please see the following link: https://ico.org.uk

What is a Subject Access Request?

If an individual makes a request for their own information, this should be considered to be a **Subject Access Request** and processed in accordance with this procedure.

Recognising a request

The GDPR does not specify how to make a valid request. Therefore, unlike under the previous Data Protection Act, a request does **not** have to be in writing, it can be made verbally. It can also be made to any part of the Council (including via social media).

A request does not have to include any specific wording such as, 'subject access request', it just has to be clear that the individual is asking for their own personal data.

Request Form

A template request form has been produced to assist individuals in making a request and also the Council in locating the relevant information. However, whilst we may invite individuals to use the template form, it is not compulsory and requests made by letter, email or verbally must still be responded to. The form can be found at www.derbyshire.gov.uk/gdpr

What is an individual entitled to?

Individuals have the right to obtain the following:

- Confirmation that you are processing their personal data and the legal basis for the processing;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom their personal information has been disclosed;
- Details of how long their information will be kept
- Any information held relating to the origin of their personal data
- A copy of their personal data; and
- Confirmation of their right to lodge a complaint with the Information Commissioner-

The request does not have to be received by a particular officer within a department to be valid. It can be sent to any Council officer. The deadline for responding will be calculated from the day following receipt (whether this is a working day or not) so it is important to ensure that it is forwarded as soon as possible to the relevant departmental contact. A list of departmental contacts is included at Appendix A and is available on Dnet - http://dnet/policies_and_procedures/access_to_information/departmental_contacts/dp_contacts/default.asp.

How information should be provided

If an individual makes a request electronically, where possible you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

Can I charge a fee for responding to a request?

In most cases you cannot charge a fee to comply with a subject access request. However, where the request is manifestly unfounded or excessive you may charge a "reasonable fee" for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies. You should seek guidance from legal services if you are considering charging a fee.

What happens if information changes from the time of the request?

The Information Commissioner's view is that a subject access request relates to data held at the time the request was received. However, in some cases routine use of data may result in it being amended, or even deleted during the time you are dealing with the request. In these circumstances it would be reasonable to supply information you hold at the time you send out the response, even if this is different to material held when the request was received.

You must not amend, or delete data relevant to the request if you would not otherwise have done so. Under the Data Protection Act 2018, it is an offence to make any amendment to information held with the intention of preventing disclosure.

When information should be provided

You must act on the subject access request without undue delay and at the latest within 1 month of receipt. You should calculate the time limit from the day after you receive the request (this includes weekends and bank holidays), until the corresponding calendar date in the next month. If this is not possible e.g. the following month is shorter and there is therefore no corresponding calendar date, the date for response is the last day of the following month. If the corresponding date is a weekend or bank holiday, the Council has until the following working day to respond. This means that the exact number of days will vary between requests. For reasons of administrative convenience you may calculate the deadline on the basis of a 28 day period to ensure your compliance date is always within a calendar month.

Extending time limits

It is possible to extend the time to respond by a further 2 months if the request is complex or the Council has received a number of requests from the same individual. You must let the individual know within 1 month of receiving their request if you intend to extend the time limit in respect of their request and you must explain to them why the extension is necessary.

Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, this must be done within 72 hours of becoming aware of the breach.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data e.g. it could include an unauthorised individual accessing records or emails containing personal data to the wrong recipient.

If you suspect that there has been a data breach you should inform your line manager as soon as possible and also record details of the suspected breach using the Service Desk Online reporting form called 'Reporting a Security Incident'

There is an icon on your computer desktop to access Service Desk online (see below)

Further information relating to data breaches is contained within the Council's Security Incident Management Policy and Procedures and Council's Practical Guide to the new Data Protection Regulation and Data Protection Act 2018. Links to both documents can be found at www.derbyshire.gov.uk/gdpr

Step by step procedure

1. A request for personal information is received by an officer at the Council. The request is emailed by the receiving officer to their Departmental Liaison Officer (DLO). If the request is made verbally a written note of the request should be taken and verified with the requester. A list of all DLOs can be found at the following link http://dnet/policies_and_procedures/access_to_information/departmental_contacts/dp_contacts/default.asp

2. The DLO logs the request.

3. The DLO considers whether it is necessary to verify the requester's identity.

4. The DLO considers whether they have enough information to locate the required data or whether it is necessary to seek further clarification from the requester.

5. After giving due consideration at steps 3 and 4 the DLO is in a position to acknowledge the request in writing. A standard letter acknowledging the request will be modified as appropriate depending on whether the DLO requires further clarification and/ or proof of identity.

6. The DLO calculates the time limit for responding to the request and logs this. The request should be responded to without undue delay and at the latest within one month of receipt, unless it is necessary to extend the time limit due to the request being complex or repeated. If the time limit is to be extended the requester must be notified of the reasons for this within 1 month of their initial request.

7. The DLO ensures that all of the personal data which is relevant to the request is gathered, either by collecting the information themselves or by liaising with the appropriate departmental officer/s.

8. After all of the information has been gathered, the officer preparing the information must ensure at this stage that third party data is redacted or the appropriate consents are sought and that all other information is removed or redacted as appropriate. (Please see guidance note 8)

9. The department must retain an electronic copy of all of the information that was considered in response to the request in an unredacted format as well as the redacted version. It is very important that it is clear what information has been withheld and which exemption has been engaged. The Departments will have their own procedure for ensuring the information is stored in a convenient location either by the DLO or the officer

preparing the information. [The Council's Electronic Data Records Management programme (EDRM) is the most efficient way of redacting the information].

10. When the information has been prepared and has been recorded as stipulated at point 8, the requester should be informed that the information is ready either to be sent out or to be collected. If the requester is collecting their information, you should ask them to sign an acknowledgement of receipt form. A template form can be accessed via this link: www.derbyshire.gov.uk/gdpr. If the requester refuses to sign this you should still provide them with their data but keep a record of their refusal.

11. Depending on the nature of the information, departments may want to invite the requester to read the records with an officer in order that the requester can discuss any concerns or questions they have about the information; this may be appropriate, for example, when viewing a social care record. However, in most circumstances the information will simply be sent to the requester's home address. Care should be taken when addressing envelopes and ensuring that it is securely packaged. If information is being supplied via email, the Council's secure email policy must be followed. A copy can be found at www.derbyshire.gov.uk/data

12. The DLO must log each completed request.

Multi-Department Requests

1. When the Council receives a SAR and the information is held by more than one department, the Access to Information Officer within the Legal Services Division will co-ordinate the response. If information is predominantly held by one Department, but that Department has received advice or support from either Human Resources or Legal Services, it shall be treated as a Single Department request.

2. If it is clear upon receipt of a SAR that the information is held within more than one department, or if it becomes clear upon receipt of clarification, the officer in receipt of the request should forward it to the Access to Information Officer (AIO) within the legal services division.

3. The AIO will consider whether any identification or clarification is required by liaising with the DLOs and will then acknowledge the request in writing. A template letter can be modified depending on whether further information is required.

4. The AIO calculates the date for response and arranges for it to be logged it on the multi-department spreadsheet.

5. The AIO sends a copy of the request to the appropriate DLOs and gives them a date upon which to forward their departments information in a redacted format. The DLO may raise with the AIO any queries relating to the disclosure of documents, but should have already completed an initial sift and carried out necessary redactions. This will be at least 7 days before the 1 month time limit expires in order to give the AIO time to check the information.

6. When each of the departments have responded in full to the AIO, the AIO will send the information to the address provided by the requester and log the SAR as complete on the spreadsheet.

Step 1 – SAR request is received by the Council

Individuals often ask for their personal data under the Freedom of Information Act 2000 (FOI). This is not the correct legislation under which to process the subject access requests as the two pieces of legislation are significantly different. It is possible to receive a request for information which should be provided under both regimes and therefore it may be necessary to consider the Council's response from a FOI perspective too. It is for the officer processing the request to inform the requester of the correct piece of legislation and the time limits that apply. If there is any doubt you should seek further guidance from Legal Services. There are a number of different ways that a SAR can be submitted to the authority. For example; a service user may phone the contact centre to make initial enquiries, in which case the contact centre may send the enquirer a form to fill out and return to the appropriate DLO. The DLO then follows the steps above. A SAR may be emailed or posted directly to the AIO within the Legal Services Division or to a social worker working directly with the requester. Any request by an individual for their personal data is a valid SAR. Regardless of where it is received it must be sent to the appropriate DLO for processing, or in the case of multi department requests – the AIO.

Step 2 – The DLO logs the request on the departmental database

It is important from a quality assurance perspective to ensure that there is a way of tracking the progress of a particular request in order that officers can be reminded of approaching deadlines and to monitor the Council's record in complying with the Council's statutory deadline. It is also important to ensure that a detailed log is kept to ensure the Council can adequately respond to any complaints made to the Information Commissioner.

Step 3 – The DLO considers whether it is necessary to verify the requester's identity

It is the enquirer's responsibility to prove that they are the data subject or that they represent the data subject. It is the Council's responsibility to ensure that requesters are required to provide appropriate proof of identity where this is necessary, before supplying information. It is important that you only ask for information that is necessary to confirm the identity of the requester. It is important to act proportionately, you need to let the individual know as soon as possible if you need more information in order to confirm their identity. The time limit for responding to the request begins from when you received the additional information.

As data controller the Council is entitled to ask for any information that officers may reasonably require to establish the identity of a requester. The DLO (or in the case of multi-department requests the AIO) should work with officers in their department to establish whether the department is providing services to the requester at the time of the SAR. If services are being provided at the time of the request, it is an 'open case'. Where the DLO is satisfied that officers know the identity and correct current address of the requester by virtue of their ongoing relationship with the Council, then there is no need to obtain further proof of identification or address. However, where there is any doubt regarding the address or identity of a requester, they must be asked to supply the documents listed below.

If, upon receipt of the request, or after communication with officers, it is clear that the requester is not receiving services from the Council at the time of the request this is a 'closed case' and more stringent identification requirements must be applied. It may be reasonable to telephone or write to the requester. The requester should in the first instance be asked to supply one form of original photo identification along with a utility bill dated within the last three months indicating their current address. Proportionality is the key consideration when establishing identity. If an individual is unable to provide originals and has a legitimate reason for this e.g. they are residing out of the area or do not have a passport or driving licence, then you should work with a requestor to see what steps may be taken to verify their identity. The DLO should use their judgement to ensure that identification

requirements do not act as barriers preventing individuals from exercising their DP rights. Processing requests on the basis of scanned identification documents may be sometimes appropriate. A passport, a photographic driving licence, or a bus pass can be used to establish identity and the electoral roll can also be used to confirm postal addresses. If requestors do not wish to send original documents by post and are unable to scan their identification documents they should be offered an appointment by the DLO to inspect their documents.

It is not necessary to retain a copy of identification documents but it is very important that a note is retained to indicate the steps taken to verify identity. Where the requester sends the original through the post, it should be inspected and logged and sent back to the requester via recorded delivery as soon as possible.

Step 4 -The DLO considers whether they have enough information to locate the required data

Occasionally requesters will make a written request for '*everything the Council holds on me*'; in these circumstances it is reasonable to ask for clarification. .In these situations it will be reasonable to write to the requester explaining that you need further information before you can begin to locate the information. You should only ask for information that you reasonably need to find the personal data covered by the request. Departments may devise a questionnaire for requesters to fill in to assist here. Where information is not held on one discreet file in the requester's name you may ask for significant dates, departments and officers.

Where the requester responds by indicating the Council will hold personal data in a number of different departments, for example, Children's Services, Adult Care and Economy, Transport & Environment, this is a multi-department request which should be processed in accordance with the procedure above.

If the DLO/AIO requires further information, it must be requested as soon as possible as delays may have to be justified to the Commissioner at a later date. The period for responding to the request begins when you receive the additional information. However, if an individual refuses to comply and provide additional information the Information Commissioner advises that you must still endeavour to comply with their request i.e. by making reasonable searches for the information covered by the request.

Step 5 – The DLO/ AIO acknowledges the request in writing

When acknowledging the initial request you should confirm the deadline by which you will respond. Alternatively, if you need identification, a fee or further information to process the request, you should make the requester aware of this as soon as possible and confirm that the response deadline will be re-calculated once you have this information. If you deem the request complex, you must also let the requester know the reasons for this within 1 month of receipt.

Step 6 – The DLO calculates the date on which the response must be provided

Requests have to be dealt with without undue delay, or within 1 month (unless complex or repeated). The time limit should be calculated from the *earliest* of the following days;

1. the day following receipt of the request, if you do not require proof of identity or clarification of what information is required* (see note 4), or

2. the date upon which you have received all of the information you require in relation to verifying the requesters identity.

Where there are unavoidable delays and it is clear to the DLO that the time limit will be exceeded then the DLO should write to the requester setting out the reason for the delay and give the requester an indication of when the Council will be in a position to provide a full response. It may be reasonable to telephone or write to the requester. If some, but not all, information relevant to the request has been obtained then the DLO should consider whether any information may be provided to the requester within the time limit, with an assurance that any outstanding information will be provided by a specified date.

Step 7 – the DLO ensures that all of the relevant information is considered

The Council has a duty to provide a requester with a copy of, or access to all structured personal data held in what is defined by the Act as held in a ' filing system'. This is drafted more widely than the previous Data Protection Act and covers any personal data held by the Council, either by manually or automated means, wherever it is located. It is only necessary to search for information that has actually been requested; e.g. if a requester has asked for information held in relation to the provision of SEN transport – it would not then be necessary to consider a social care file or information held within the Community Safety or Emergency Planning divisions. You are not required to produce information which has been destroyed prior to the receipt of a request.

Relevant information should never be destroyed after a request has been received. If you are seeking clarification from the requester to help locate their information it may be helpful to establish:

- where the requester thinks that their information is likely to be held;
- the names of the authors and recipients of any messages;
- the subject line of the e-mails;
- the dates, or range of dates, on which the messages were sent;

After searching central manual and computerised files, the DLO may need to send a request around the section or department asking people to search their own records for information about the individual. Please remember that the purpose of the search is to uncover all the information that we hold, as a Council, about the individual. More detailed searches at this stage are likely to result in fewer queries and complaints afterward.

The GDPR requires that the information provided to an individual is in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Essentially, this means that the information provided in response to a request should be capable of being understood by the average person (or a child). If when preparing a response to a subject access request you notice that a lot of information is in coded form which would make it impossible for those outside the Council to understand you should explain the meaning of it. You are not legally required to decipher poorly written notices but as a matter of good practice if possible you should do this.

Step 8 – The information is prepared

There are some types of information that the Act says you do not have to provide when responding to a subject access request such as some information relating to third parties. Legal advice should be sought if you are not sure whether to apply an exemption. Further detailed guidance in relation to relevant exemptions will be provided in due course.

Where the requested information includes personal data relating to another individual (a third party), you need to consider whether to release that information to the enquirer. There are three actions you can take.

1. You can obtain the third party's consent to the disclosure, if it is reasonable to do so, or

2. you can edit the information so as not to reveal the third party's identity, for example, blocking out the text or retyping text without the identifying information; or

3. You can decide that it is reasonable to disclose the information to the data subject without the third party's consent.

In taking this third option you need to consider:

- the type of information you would disclose
- any duty of confidentiality owed to a third party
- any steps you have taken to obtain consent;
- whether the third party is capable of giving consent;
- whether the third party has expressly refused consent;
- whether the information is of particular importance to the data subject.

For the purposes of data protection, references to DCC officers carrying out their professional roles and duties and records of their professional assessments, statements or opinions are not generally considered to be third-party data.

If is it not reasonable, or possible to obtain consent; often, third party data can be redacted using the Council's EDRM system. This system allows the preparing officer to conceal third party information and clearly mark it as *'third party data*'. Where it is impossible to extract one person's personal data from another individual's personal data, the officer should consider whether it is appropriate to provide the requester with a summary of their information. Extracting one person's data from that of a third party can be particularly difficult when considering complaints files and files held within the Council's social services departments. The departmental DLO and the Legal advisors will be able to assist with this if there is any doubt and there is a lot of useful guidance on the Information Commissioner's website.

Files will occasionally contain information which has been created by another organisation. For example; a social services file may contain information from health workers and general practitioners. Where the information relates to the mental or physical wellbeing of the data subject and it is created by a Professional who does not work for DCC, where possible the health worker should be contacted to obtain their views about disclosure. This should be recorded by the DLO/ officer preparing the file. This may be more difficult where the SAR relates to a 'closed case' as it may be more difficult to contact the health professionals. The officer preparing the information should take a view on whether it is appropriate to disclose that particular piece of information, in the absence of consent from the third party. Any officer preparing a social services files for disclosure should familiarise themselves with the guidance provided by the Information Commissioner for regarding the disclosure of social services files.

Refusing to comply with a request

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

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 it. However, in either case you will need to justify your decision and confirm the reasons for this to the requester. If you decided to charge a fee you do not need to comply with the request until this has been received.

Further guidance in relation to individual exemptions will be provided once the Data Protection Act has been finalised and reviewed.

Step 10 – Finalising, recording and retaining the progress of the SAR

It is important that the DLO is sent a copy of the response if they are not the officer responsible for preparing the information. The DLO will record the request as complete when they have sent the information to the requester or the responding officer has sent the DLO a copy of their response. Again, it is important to retain an electronic copy of the information that was considered as well as a copy of any information that was withheld in full or redacted. A clear record should be kept explaining the legal basis upon which each document/ section of the document was withheld and whether information was sent by email, post or collected. The most efficient way to do this is using the Council's EDRM system. All correspondence between the DLO and the enquirer should also be retained. This is necessary because the information may been needed internally as part of a complaints investigation or audit, or externally, as part of an investigation by the regulator.

This information should usually be retained for a period of 3 years from the closure of the case, unless it is copied to an individual file in which case it will be saved in accordance with the relevant published retention schedule.

Please note that the regulator, the Information Commissioner, is duty bound by law to investigate all complaints made in relation to an organisations handling of personal data.

It is important that a request is marked as complete for quality assurance purposes and to allow the DLO to chase up overdue requests. DLO's should maintain records of SAR compliance rates.

Step 11 Cold Case Reviews

In order to ensure that subject access requests are dealt with consistently and in line with best practice, the DLO will ensure that 2 cold case reviews will be carried out each quarter on cases that the DLO has not had involvement in. The results of these will be fed back to the Information Implementation Group (IIG) and reported to the Information Governance Group via the IIG minutes.

Requests made on behalf of others

Subject access requests can be made on behalf of others e.g. a solicitor may request information on behalf of their client, other individuals may feel more comfortable with the request being made by someone else acting on their instructions. In these cases you must be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the responsibility of the person making the request to demonstrate that they are making the request on behalf of the individual. This could be via a written authority from the data subject or a power of attorney.

If you think that an individual may not understand what information would be disclosed to a third party who has made a subject access request on their behalf you may send the information directly to the data subject in order that they can then decide whether to share it once they have had the opportunity to review it.

Other organisations can also make requests for personal data such as the Police, the Inland Revenue, the Audit Commission or a court, these are not Subject Access Requests and are therefore not dealt with under this procedure.

Other institutions can also make requests for personal data, such as the Police, the Inland Revenue, the Audit Commission or a court. These are not Subject Access Requests and are therefore not dealt with under this procedure.

Requests for educational records held by schools

Different rules apply to educational records and these should also be considered under the Education (Pupil Information) (England) Regulations 2005. The definition of an educational record is wide and includes: any information which is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local authority and any special school which is not maintained; relates to any person who is or has been a pupil at any such school; originated from or was supplied by or on behalf of any employee of the local authority which maintains the school or former school attended by the pupil to whom the record relates; in the case of a voluntary aided, foundation or foundation special school or a special school which is not maintained by a local authority, a teacher or other employee at the school or at the pupil's former school (including any educational psychologist engaged by the governing body under a contract for services); the pupil to whom the record relates; and a parent of that pupil. It therefore includes the curricular record and also includes:

- Any education, health and care (EHC) plan, formerly a statement of special educational needs.
- Any personal education plan.

Educational records do not include information which is processed by a teacher solely for the teacher's own use, such as lesson plans.

Requests for information about children

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child to make a request rather than anyone else such as a parent or guardian. In the case of young children, this is likely to be exercised by those with parental responsibility.

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

When considering borderline cases, you should take into account, amongst 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 consequence 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;
- Any views of the child or young person has on whether their parents should have information about them

If you are offering an online service directly to children on the basis of consent, then the Data Protection Act 2018 specifies 13 years old as the appropriate age of consent.

Requests for Occupational Health Records

The Council's Occupational Health Unit holds health information about employees, former employees and prospective employees. You should direct the requester to occupational health if they want information held by that department.

Requests for archival records held by the Derbyshire Record Office

Historical archives held at the Record Office may be held by Derbyshire County Council on behalf of another organisation, with different access requirements and an external Data Controller, depending on the type of material and which organisation deposited the records. Subject Access Requests relating to archives at the Record office will be managed by the Duty Archivist. The National Archives August 2018 Guide To Archiving Personal Data, is available here http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/

Complaints

All complaints about subject access must be immediately notified to the Access to Information Officer (AIO) who will determine the appropriate next steps. The AIO maintains a record of all requests for internal reviews and complaints which are escalated to the Information Commissioner's Office. This data is shared with the Council's Data Protection Officer and reported to the Council's Information Governance and Implementation Groups to facilitate trend analysis and improve working practice.

Appendix A

Department SAR Contact Details

For internal DCC Staff Only

Details of Departmental Contacts for Subject Access Requests can be found on Dnet at:
http://dnet/policies_and_procedures/access_to_information/departmental_contacts/dp_contacts/default.asp

This document is owned by the Information Governance Group and forms part of the Council's ISMS and as such, must be fully complied with.