From: Foi Enquiries
To: [redacted]
Subject: FOI-16-0719 - Data Protection Breaches
Date: 08 July 2016 15:16:00
Attachments: Further Information - Right to Review & Appeal.pdf
FOI-16-0719 - Corporate Data Protection Policy.pdf
FOI-16-0719 - data protection corporate reporting form.doc

Dear [redacted],

Your Reference: [redacted]

Please accept our sincere apologies for the delay in responding to your information request of 23 May 2016. Aberdeen City Council (ACC) has completed the necessary search for the information requested.

I am writing under the Freedom of Information Act 2000 to request details of breaches of the Data Protection Act within in your organisation; specifically I am asking for:

1a. Approximately how many members of staff do you have?
8,996 as at 26 May 2016.

1b. Approximately how many contractors have routine access to your information?
In total, approximately 100 contractors will have (or have had) access to certain information held by ACC. This can be for a variety of reasons and may be only for a certain amount of time while completing a certain project. Under our duty to advise and assist please see below some details of access provided.

One printer has access to the mailing list for Newsbite magazine published 3 times a year.
Northgate has access to certain information.
There can be a maximum of 150 third party users who would have read-only access limited view of our Carefirst system – these would be users from Bon Accord Care and NHS.
Only one member of staff who is the Housing OT who works within Communities Housing and Infrastructure but is employed by Bon Accord Care which is a Local Authority Trading Company Civica in relation to the APP system (and in future IDOX for the Uniform system).

Housing Support Contracts
Aberdeen Cyrenians
Deafblind Scotland
Cornerstone
Turning Point Scotland
Blackwood Homes
Grampian Autistic Society
Penumbra
Castlehill Key Project
Grampian Women's Aid
SAMH

Inspire
Aberdeen Foyer
Sheltered Housing
Hanover Housing Association
VSA
Castlehill
Sanctuary Housing
Housing Advice
Instant Neighbour
Shelter
Barnardos
AUs/PSL.TFF
The Furnishing Service
Goldstar Cleaning
ACC Cleaning
Bon Accord Support Services
Other
Huddle

The company contracted to provide external hosting of ACC web servers would have access to ACC information, in a managed and regulated manner through contractual agreement. We do not hold information on how many contractors this would be.

Contractors who have to provide support and maintenance for some applications are set up with a dedicated managed secure VPN tunnel and are only allowed access once they have followed the IT Change Control process e.g. help desk call logged with a change control form completed, stating what work is being done, when and for how long. Once work has been completed the secure VPN tunnel is disabled. There are approx. 70 vendors.

2a. Do you have an information security incident/event reporting policy/guidance/management document(s) that includes categorisation/classification of such incidents?

Aberdeen City Council has a Corporate Data Protection Policy. Data Protection breaches are classified as:

- Human Error
- Loss
- Theft
- Unauthorised disclosure
- Unauthorised access
- Unauthorised use

2b. Can you provide me with the information or document(s) referred to in 2a? (This can be an email attachment of the document(s), a link to the document(s) on your publicly facing web site or a 'cut and paste' of the relevant section of these document(s))
Please find attached Aberdeen City Council's Corporate Data Protection Policy and Corporate Reporting Form as approved by the Finance, Policy and Resources Committee of 15 September 2015.

3a. Do you know how many data protection incidents your organisation has had since April 2011? (Incidents reported to the Information Commissioners Office (ICO) as a Data Protection Act (DPA) breach)
Answer: Yes, No,
Only since (date):
Yes

3b. How many breaches occurred for each Financial Year the figures are available for?
Answer
FY11-12: 1
FY12-13: 0
FY13-14: 2
FY14-15: 2

4a. Do you know how many other information security incidents your organisation has had since April 2011? (A breach resulting in the loss of organisational information other than an incident reported to the ICO, eg compromise of sensitive contracts or encryption by malware.)
Answer: Yes, No, Only since (date):
Yes, loss is one of the categories that Aberdeen City Council records data protection breaches.

4b. How many incidents occurred for each Financial Year the figures are available for?
Answer
FY11-12: 2
FY12-13: 2
FY13-14: 4
FY14-15: 1

5a. Do you know how many information security events/anomaly your organisation has had since April 2011? (Events where information loss did not occur but resources were assigned to investigate or recover, eg nuisance malware or locating misfiled documents.)
Answer: Yes, No, Only since (date):
No, we do not specifically record events where information loss did not occur but resources were assigned to investigate or recover. We record any data protection breach as human error, loss, theft, unauthorised disclosure, unauthorised access and unauthorised use.

ACC is unable to provide you with information on **how many information security events/anomaly your organisation has had since April 2011** as it is not held by ACC. In order to comply with its obligations under the terms of Section 17 of the FOISA, ACC hereby gives notice that this information is not held by it.

5b. How many events occurred for each Financial Year the figures are available for?
Answer FY11-12: FY12-13: FY13-14: FY14-15:
Not applicable, please see our answer above.

6a. Do you know how many information security near misses your organisation has had since April 2011? (Problems reported to the information security teams that indicate a possible technical, administrative or procedural issue.)
Answer: Yes, No, Only since (date):
Yes, Aberdeen City Council keeps a record of data protection near misses.

6b. How many near-misses occurred for each Financial Year the figures are available for?
Answer FY11-12: 0 **FY12-13:** 0 **FY13-14:** 0 **FY14-15:** 0

For further information, please see the committee report at the following link. Contained within the papers is a Data Protection report for 2015/16.

http://committees.aberdeencity.gov.uk/documents/g3914/Public%20reports%20pack%2027th-Jun-2016%2014.00%20Audit%20Risk%20and%20Scrutiny%20Committee.pdf?T=10

We hope this helps with your request.

Yours sincerely,

Grant Webster
Information Compliance Officer

INFORMATION ABOUT THE HANDLING OF YOUR REQUEST

ACC handled your request for information in accordance with the provisions of the Freedom of Information (Scotland) Act 2002. Please refer to the attached PDF for more information about your rights under FOISA.

Information Compliance Team
Communications and Promotion
Office of Chief Executive
Aberdeen City Council
Room 1-24
Town House
Broad Street
ABERDEEN AB10 1AQ

foienquiries@aberdeencity.gov.uk
01224 523827/523602

Tel 03000 200 292

*03000 numbers are free to call if you have 'free minutes' included in your mobile call plan.

Calls from BT landlines will be charged at the local call rate of 10.24p per minute (the same as 01224s).

www.aberdeencity.gov.uk

New Corporate Data Protection Policy

Table of contents

APPENDIX ONE – DATA PROTECTION POLICY

Corporate Data Protection Policy

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1.0	15th September 2015		Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1. Introduction

1.1 In order to perform their role, Staff and Elected Members of Aberdeen City Council (ACC) necessarily use a vast amount of personal information about citizens, customers, staff, suppliers and other individuals.

1.2 The Data Protection Act 1998 (DPA 1998) is legislation which applies to all organisations and individuals in the UK who are defined as a Data Controller. A Data Controller is a body or person who determines how personal information is to be used. For the purposes of the DPA 1998, ACC is registered as a Data Controller.

1.3 The DPA 1998 incorporates, as Data Protection Principles, the rules of good information handling practice. In addition, the spirit of the DPA 1998 is to help to secure an individual's right to privacy. As such the DPA 1998 sets out the standards which must be applied by ACC in the handling of personal information.

1.4 This Corporate Data Protection Policy and the associated Data Protection procedures highlighted within it outline the manner in which ACC will meet the

obligations and duties which the DPA 1998 sets out. These corporate documents will be supported with Service specific procedures where necessary.

2. Personal Information

2.1 Personal Information is defined as information which:

a) relates to a living individual

AND

b) the individual can be identified from that information alone or in conjunction with other available information.

2.2 A living individual about whom personal information is held is known in the DPA 1998 as the Data Subject.

2.3 The terminology in the DPA 1998 for the use of Personal information by a Data Controller is that personal information is processed. The definition of processing is very wide and it is likely that all activities undertaken by ACC using personal information will be captured by it, including obtaining, recording or holding the information and carrying out any operation or set of operations on the information or data, such as organising, adapting or altering the information; retrieving, consulting or using the information; disclosing the information by transmitting, disseminating or otherwise making available, or aligning, combining, blocking, erasing or destroying the information.

2.4 The DPA 1998 provides for additional measures to be taken in respect of sensitive personal information, this being information relating to a Data Subjects:

i) Race;

ii) Political opinions;

iii) Religious beliefs or other beliefs of a similar nature;

iv) Trade Union membership;

v) Physical or mental health;

vi) Sexual life;

vii) Commission or alleged commission of any offence, including any proceedings for any offence committed or alleged to have been committed by him and the disposal of such proceedings or the sentence of any court in such proceedings.

3. Data Protection Principles

3.1 ACC is committed to processing personal information fairly and lawfully at all times and therefore fully endorses and adheres to the eight principles of Data Protection as set out in the DPA 1998.

3.2 The eight Data Protection principles require that personal information is:

i) Processed fairly and lawfully and in particular, is not processed unless certain conditions can be met.

ii) Obtained only for one or more specified and lawful purpose, and not further processed in any manner incompatible with that purpose or those purposes.

iii) Adequate, relevant and not excessive for the purpose(s) for which it is processed.

iv) Accurate and, where necessary, kept up-to-date.

v) Not kept for longer than is necessary

vi) Processed in accordance with the rights of data subjects, these being:

- The right to access the data held about them;
- The right to prevent processing likely to cause damage or distress;
- The right to prevent processing for the purposes of direct marketing;
- The right to object to automated decisions being taken about them;
- The right to claim compensation for damage or distress caused by a breach of the DPA 1998;
- The right to apply for rectification, blocking or erasure of inaccurate data.

vii) Protected by appropriate technical and organisational measures to prevent unauthorised or unlawful processing and to prevent accidental loss, destruction or damage.

viii) Not transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

3.3 Sections 6 and 7 of this policy provide further detail, and links to applicable procedures, relating to each of these principles.

4. Corporate Data Protection Framework

4.1 In order to meet its obligations under the Data Protection principles, ACC have in place a clear framework of roles and responsibilities including training and support provided to all staff and Elected Members.

4.2 All Staff and Elected Members

4.2.1 All Staff and Elected Members will, as part of their induction to ACC, be introduced to the Data Protection principles, made aware of their responsibilities and obligations under this policy and its associated procedures and be signposted to further sources of training, guidance and support within ACC on data protection matters.

4.2.2 Where poor handling of personal information by any individual is identified, appropriate steps to provide training and support to address the reasons for such performance will be provided at the earliest possible opportunity.

4.2.3 Any deliberate and/or wilful breach of this policy may lead to disciplinary action being taken and may be reported to the Police.

4.3 Elected Members and Staff with a Job Profile identified as being one which processes Personal Information

4.3.1 Staff and Elected Members who, as part of their job or role, undertake the processing of personal information will be required to undertake specified Data Protection Training at the commencement of their employment / office and to undertake specified Refresher Training at appropriate intervals thereafter. This training will provide a detailed overview of Data Protection principles, policy and procedures.

4.3.2 All Staff and Elected Members who are responsible for managing and handling personal information have a contractual responsibility to follow good data protection practice and to adhere to all Data Protection policies and procedures adopted by ACC. A duty to safeguard the security and confidentiality of personal information accessed by virtue of the role extends to Staff and Elected Members both throughout and following the end of their term of employment / term of office.

4.3.3 Any member of Staff or Elected Member who has a query about the handling of personal information must contact the relevant Service Information Management Liaison Officer (IMLO) in relation to that query.

4.3.4 Any query received by a member of Staff or Elected Member from a data subject with respect to the handling of their personal information must be dealt with in a prompt and courteous manner and, in particular, timeously in accordance with the timescales specified in the DPA 1998.

4.4 Information Management Liaison Officers (IMLO's)

4.4.1 Each Service within ACC will nominate at least one Information Management Liaison Officer (IMLO).

4.4.2 IMLO's are responsible for providing support to all staff within their Service with respect to any Data Protection queries and any member of Staff with a query regarding Data Protection should, in the first instance, contact their Service IMLO. Contact details for all IMLO's are accessible via the Data Protection pages on the Zone.

4.4.3 IMLO's will receive specialised training on issues of Data Protection law, its implications for ACC and ACC Data Protection policy and procedures and can obtain legal advice and assistance on request from Team 2, Commercial ^ Advice, Legal Services.

4.4.4 Regular IMLO meetings will be held at which changes in law and practice and any concerns in respect of ACC's compliance with this policy and the associated procedures will be discussed.

4.5 Data Protection Technical Officer (DPTO)

4.5.1 A DPTO will be appointed by the relevant Service to deal with matters pertinent to ICT and Data Protection. Contact details for the current DPTO will be available on the Zone.

4.6 Commercial & Advice Team – Legal Services (Team 2)

4.6.1 Solicitors and other staff employed within Team 2 of the Commercial & Advice Team of Legal Services provide detailed advice and assistance on Data Protection matters across ACC.

4.7 Head of Legal & Democratic Services

4.7.1 The Head of Legal & Democratic Services (Head of LADS) is the Nominated Representative of the Data Controller in terms of the DPA 1998. In addition the Head of LADS is nominated as the ACC Data Protection Officer.

4.7.2 The Head of LADS has overall responsibility for this Data Protection policy and the associated procedures and will review each on a regular basis to ensure any revised guidance from the Information Commissioner or changes within the law are incorporated within them.

4.8 All Heads of Service

4.8.1 Each Head of Service is ultimately responsible for the adherence of this policy and the associated procedures by their staff.

4.9 Elected Members

4.9.1 Elected Members have an ultimate governance role in overseeing the adherence of ACC to its Data Protection obligations. In practice, this role is discharged via the submission of quarterly Data Protection Monitoring reports to the appropriate Council Committee.

5. Data Protection Registration

5.1 ACC is registered with the ICO as a Data Controller. The current registration can be accessed on the ICO's website and provides an overview of the types of personal information processed by ACC and the purposes for which personal information is processed are detailed within the registration.

5.2 The registration is updated on an Annual basis and will be co-ordinated by Officers from Team 2, Commercial & Advice Team, Legal Services on behalf of the ACC Data Protection Officer who will liaise with the DPTO and Services to confirm if there has

been any change in the preceding year of the categories of personal information processed or the purposes of processing,

5.3 Individual Elected Members have their own responsibility for registering as a Data Controller for those matters for which they process personal information which are not directly related to ACC business and which are therefore not covered by ACC's notification. Further information and advice on this requirement is available to Elected Members via Members Support in the first instance.

6. Lifecycle of Personal Information

6.1 Collecting Personal Information

6.1.1 ACC will only collect personal information about individuals where it is necessary to do so in order that operational / service needs can be fulfilled. Particular care will be taken to ensure that no sensitive personal information is collected unless doing so is necessary for the purposes that information is sought.

6.1.2 Personal Information can be collected in a variety of ways, for example, by requesting a data subject completes an application form for a service, by inviting data subjects to complete a questionnaire or by speaking to data subjects and capturing their responses. Personal information can be gathered electronically or via paper based methods.

6.1.3 At all times that ACC collects personal information an appropriate Privacy Notice must be used in order to:

- advise Data Subjects what personal information is being collected;
- advise what the personal information will be used for;
- advise who, if anyone, the personal information will be shared with;
- advise individuals of the Officer who can be contacted with any query and how any objection to processing can be made.

6.1.4 A template Corporate Privacy Notice is available in the Corporate Data Protection – Collecting Personal Information procedure.

6.2 Using Personal Information

6.2.1 Personal Information will only be used by ACC for the purposes for which it was collected unless there is a lawful reason to use it for any other purpose.

6.2.2 Whilst using personal information, Staff and Elected Members must take appropriate steps to protect and safeguard the security of the information and to ensure that no person who is not authorised to access it is able to do so.

6.2.3 Staff and Elected Members must only access and use personal information stored by ACC for the purposes of work carried out on behalf of ACC.

6.3 Storing Personal Information

6.3.1 All personal information collected and stored by ACC must be stored in adherence to applicable Council procedures to ensure it is kept in a manner which safeguards the security of the information and prevents unauthorised access to it.

6.3.2 Appropriate technical and organisational security measures will be implemented and regularly monitored to ensure the security of personal information stored by ACC is safeguarded.

6.4 Sharing Personal Information

6.4.1 Personal Information held by ACC will only be shared across services or externally where it is appropriate to do so. The process for sharing of personal information is detailed in the ACC Corporate Data Protection Procedure – Sharing of Personal Information.

6.5 Access to Personal Information

6.5.1 ACC recognises that it is a fundamental right of Data Subjects to access the personal information held about them. The procedure for handling any Subject Access Request received is detailed in the ACC Corporate Data Protection Procedure – Access to Personal Information (Subject Access).

6.5.2 The ACC Corporate Data Protection Procedure – Access to Personal Information (Third Party Access) sets out those instances where ACC will provide access to personal information to other agencies. Staff and Elected Members must be aware of these procedures and ensure access to personal information is only provided in line with these.

6.6 Disposing of Personal Information

6.6.1 All personal information will be disposed of securely and in line with applicable information retention policies. Further guidance on retention and disposal of information can been accessed in the Corporate Records Retention Policy.

7. When Things go Wrong

7.1 ACC recognises that due to human or system error, there will be occasions when the security of personal info may be breached. A robust system for the reporting,

management and investigation of such breaches is in place and all Staff and Elected Members are obliged to report such matters without delay. The procedure for reporting such matters is set out in the 'ACC Corporate Data Protection Procedure – Reporting of Data Protection Incidents' document.

7.2 In addition, ACC is committed to the reporting and recording of Data Protection Near Misses. A Near Miss is defined as an unplanned occurrence which did not ultimately lead to a data protection breach occurring but had the potential to. The procedure for the reporting of near misses is also detailed in the 'ACC Corporate Data Protection Procedure – Reporting of Data Protection Incidents' document.

7.3 Regular monitoring of Data protection incidents by Team 2, Commercial & Advice Team, Legal Services will be undertaken and any trends or patterns identified will be advised to Services for appropriate system / procedure review and reported to Elected Members via quarterly Data Protection reports to the Audit, Risk & Scrutiny Committee.

7.4 ACC is committed to a culture which encourages early identification of data protection incidents and which provides appropriate training and support to individuals involved. Notwithstanding this, ACC will, where deliberate or wilful behaviour leads to a data protection incident take appropriate disciplinary action and/or report the matter to the police.

8. Review

8.1 The ACC Corporate Data Protection Policy and Procedures will be reviewed by Legal Services Staff on at least an annual basis or as a consequence of any change in Data Protection Law.

APPENDIX TWO - CORPORATE CREATING PERSONAL INFORMATION PROCEDURE

Corporate Data Protection Procedure –

Collecting Personal Information

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1.0	15th September 2015	-	Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1. Introduction

1.1 The purpose of this procedure is to set out the manner in which personal information should be collected by ACC. It is intended to be used by any ACC Staff involved in the development and operation of processes for collecting personal information.

2. Collecting Personal Information

a. The collection of personal information must be done fairly and lawfully. A key part of fairness is ensuring that people know how their information will be used by ACC.

b. The basic requirements to ensure that collecting personal information is fair is to make sure people know:

- **Who** is collecting the personal information

- **Why** the personal information is being collected – or, in other words, **what** will be done with it
- **Who**, if anyone, the personal information will be shared with.

Other requirements, which, depending on the individual circumstances, may be necessary include:

- **How** long the personal information will be kept
- Whether providing the personal information is **voluntary** or **mandatory**
- Any **consequences** to the individual if the personal information is not provided
- **What** arrangements are in place to ensure the security of personal information
- **Who** can be contacted if the individual wishes to exercise their rights or complain about the way their personal information is used

c. Individuals have a fundamental right to know how their personal information will be used; therefore ACC must be transparent and truthful when collecting personal information about how it will be used.

d. Where individuals have a choice whether to provide their personal information or not, this must been clear in order that a genuine opportunity is provided to refuse to do so.

3. Privacy Notices

a. A Privacy Notice is a statement which tells data subjects who is collecting their personal information, why it is being collected and who, if anybody, if will be shared with. The purpose of a Privacy Notice is to make sure that personal information is collected fairly.

b. A Privacy Notice should be clear and simple to understand. There is no 'one size fits all' notice which captures all of the functions undertaken by ACC and having notices aimed at the different groups of people personal information is collected from can make it easier for people to understand.

c. When drafting a privacy notice, the opportunity should be taken to review the collection of information, for example, by asking if it is really necessary to gather the information that is being asked for.

d. There are many ways in which a privacy notice can be displayed and the appropriate manner will depend on the nature of the information being gathered and the way in which it is collected. A Privacy Notice can be provided orally (face to face or via telephone); in writing, through signage being displayed or electronically. It is good practice to use the same mode that is used to collect the personal information to deliver the privacy notice, for example if an application form is used it is good practice to print the privacy notice on it, whereas if an internet comments form is used it is good practice to host the privacy notice online.

e. Where personal information is collected from individuals who have specific communication needs such as children, disabled people and those for whom English is not a first language, it is a requirement that efforts to draft suitable Privacy Notices take account of those specific needs.

f. Good practice states that Privacy Notices should be regularly reviewed in order to ensure that they are up-to-date and relevant and reflect any changes in the way in which personal information is gathered.

g. The exact contents of a Privacy Notice will vary depending on the nature of the personal information being collected. However, as a guide, a Corporate Privacy Notice template has been developed and is shown in Appendix A.

4. Sources of Further Information and Assistance

a. Further information about Privacy Notices is available on the Data Protection page of the Zone where a copy of the ICO Guide 'Privacy Notices: Code of Practice' is available.

b. Assistance in respect of Privacy Notices can be requested in the first instance from the Information Management Liaison Officer (IMLO) for each Service who can request input from Legal Staff if needed.

Appendix A – Corporate Style Privacy Notice

Using your personal information

Information you supply to Aberdeen City Council (ACC) within this **[*1]** will/ may **[*2]** be used **[*3].**

ACC may share your information with …and/or obtain information about you from **[*4].**

ACC will not disclose any information about you to any organisation or person unless it is authorised or required to do so by law.

[*optional*] For further information on how your information is used, how ACC maintain the security of your information, and your rights to access information ACC holds about you, please contact **[*5]**

[*1] Insert what media the information is collected by, e.g. in writing (form, printed adverts or online web form), posters, text messages, on websites or by email.

[*2] Delete which does not apply. In some cases the information you collect will be clearly for one defined purpose, however there may be situations where the information you collect could be used for a number of related or unrelated purposes. Where the person would not reasonably expect to you use the information for the purpose you intend you should make it clear in your notice.

[*3] Include here a short description of the purpose(s) for which you will use the information e.g. "for fraud prevention, for audit and debt collection".

[*4] Include here who the information will be disclosed to e.g any other party/organisation. You should also advise if the information is to be used for any additional purposes e.g. to contact the person again in the future. You may have to provide the person with an opportunity to object to their information being used in a certain way.

[*5] Insert web address to Access to Information Pages, or contact name and address it's always best to include something in the form which enables the person to obtain further information. However, there may already be a process for this on the form or website

APPENDIX THREE - CORPORATE ACCESS TO PERSONAL INFORMATION (SUBJECT ACCESS) PROCEDURE

Protection Procedure – Access to Personal Information (Subject Access)

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1.0	15th September 2015	-	Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1. Introduction

1.1 The purpose of this procedure is to outline the way in which requests received by Aberdeen City Council (ACC) for access to the personal information it holds should be handled.

1.2 The way in which requests for access to personal information are handled depends on who makes the request and care should be taken to ensure that the correct procedure is followed.

- Where a request is received from the data subject (the person about who the information relates) or from someone acting on the data subjects behalf, the request is a **Subject Access Request** (See section 2).
- Where a request is received from a person other than the data subject or his representative or from another organisation / agency, the request should be handled as a **Third Party Request for Personal Information** (See Access to Information – Third Party Procedure).

2. Subject Access Requests (SARs)

Section 2.1: What is Subject Access?

2.1.1 Subject Access is a fundamental right of data subjects. In other words, all data subjects about whom ACC hold personal information, have a right to access that information. It is therefore good practice to promote rights of Subject access and to encourage and support individuals to make use of these.

2.1.2 A Subject Access Request (SAR) is a request by a data subject to access their personal information. A SAR should be made in writing, but can be made in any format including e-mail, letter, social media, fax, etc. A request does not need to be on any specific form or even to mention it is a SAR, only to state that access to the information is requested.

2.1.3 An oral request can, depending on the circumstances in which it is made, be responded to. If responding to an oral request, care must be taken as to check the identity of the requester and the information they wish to access.

2.1.4 ACC may receive a Freedom of Information (FOI) request from a data subject for access to their personal information. This will be passed on to the relevant service for handling as a SAR.

2.1.5 Before responding to a request, the requester can be asked for clarification of the information being sought if this is necessary to assist with locating it within ACC records. Such clarification must be requested promptly. The timescale for responding to the request does not commence until clarification requested is received.

2.1.5 A SAR gives individuals the right to access only personal information about themselves; it does not give a right of access to the personal information of other people. Any such request should be handled as a Third Party Request for Personal Information (See Section 3).

2.1.6 A SAR does not require to made to any specific point of contact within ACC and can be submitted to any member of staff. A SAR should be handled by the most appropriate officer within the Service to which it is directed. This may be the Case Officer, the Service Information Management Liaison Officer (IMLO) or a Service Manager. Where a SAR covers more than one Service, IMLO's from each Service involved should identify whether a single ACC response or separate Service responses will be made.

Section 2.2: Who can make a SAR?

2.2.1 A SAR can be made by the Data Subject or by a person acting on behalf of the Data Subject. The representative may be a solicitor or other professional, an advocate or other support person or any other person who the data subject wishes to act for them.

2.2.2 In cases where the SAR is made by the Data Subject, ACC requires to be satisfied of the identity of the person making the request. As such, it may be necessary to request proof of identity (e.g: driving license, passport, proof of address). ACC requires to be reasonable in accessing what proof of identity is necessary depending on the specific circumstances of the request. If the requester is generally known to the person to who the request is made it is unlikely that formal proof of identity would be required. If proof of identity is required, this must be requested promptly and the timescale for response does not commence until it is received.

2.2.3 In cases where the SAR is made by a person acting on behalf of the Data Subject, ACC requires to be satisfied both of the identity of the Data Subject and that the person making the request is entitled to act on behalf of the Data Subject. This could be through a signed mandate or more formal power of attorney, sight of which should be requested in order to evidence this power.

2.2.4 The personal information held by ACC about children is the child's personal information and it is the child who has a right of subject

access. The law in Scotland presumes that a child aged 12 and over has capacity to make its own SAR. As such, a parent or guardian can only exercise rights of subject access to personal information about a child older than 12 with the consent of the child. For children aged under 12, a parent or guardian can exercise rights of subject access on behalf of a child.

Notwithstanding this position, a parent / guardian of a school pupil has the right to access the pupil's educational record irrespective of the age of the pupil. For more details see Section 2.5 of the ACC Corporate Data Protection Procedure - Access to Information (Third Party Procedure).

Section 2.3: Time Limits and Fees

2.3.1 A SAR must be responded to within 40 calendar days of the latest date of:

- Receipt of the request
- Receipt of the fee (if charged)
- Receipt of proof of ID (if requested)
- Receipt of any clarification requested to help locate the information.

2.3.2 There is no provision to extend this deadline and every effort must be made to meet it. ACC is in breach of its obligations under the Data Protection Act if the timescale is not met and the Data Subject can request the Information Commissioner investigate this. If there is any delay in responding to the request and this timescale cannot be met, it is good practice to advice the requester of this and to keep the requester updated of the estimated timescale for response.

2.3.3 ACC can charge a fee for handling a SAR. The maximum fee that can be charged is £10. Individual services have Service Guidance to determine whether or not a fee will be charged. Where a fee is charged this should be recorded as income to the Services General Administration budget.

2.3.4 If a fee is to be charged and is not included with the initial request, payment must be requested promptly. The 40 day timescale for responding to a SAR does not commence until the payment is received but, once the request is being processed, ACC cannot decide to charge a fee where this was not done initially merely to extend the timescale.

Section 2.4: Finding and Retrieving Information

2.4.1 There is no exemption which enables ACC to refuse to respond to a SAR due to the extent of information requested or the effort required to prepare the response. In addition, a requester cannot be asked to narrow the request to make it easier to respond to. As such, it may be that extensive efforts are required to find and retrieve the information requested.

2.4.2 Information which is archived is also captured as part of a SAR and therefore services should have in place processes to allow for archived information to be retrieved and supplied in response to a SAR.

2.4.3 Information which has been deleted is not captured by a SAR. Where electronic information has been deleted, it is not necessary to take steps to recover that information, even if this would be possible if appropriate technical knowledge and skills were applied.

2.4.4 The information requested by a SAR is the information as it exists on the date the request is received. However, routine maintenance of the data can still be done, so long as this would have been done even if the request was not received. It is good practice to provide

the most up-to-date records in response to a request. However, it is not permissible to amend data as a result of receiving the SAR if it would not otherwise been done.

2.4.5 If the information exists in an 'unstructured filing system', in other words information which is not in a filing system of some kind, there may be a cost exemption which applies if searching for the information would take in excess of 18 hours. This is a very narrow exemption which can rarely be used. The cost calculation must be undertaken prior to the information being searched for. Specific advice on the application of this exemption can be obtained from Legal Services (Team 2, Commercial & Advice).

Section 2.5: Third Party Information

2.5.1 The information captured by a SAR may also include personal information of others, including other customers / clients and staff members. Rights of subject access allow people to access their own information only therefore it is not necessary comply with a SAR if to do so would mean disclosing personal information about a 3rd party, except where:

- The 3rd party has consented to the disclosure; or
- It is reasonable in all the circumstances to comply with the SAR without the 3rd party's consent.

2.5.2 Decisions in respect of 3rd party information must be made on a case by case basis, with advice being sought from the IMLO / Legal Services if necessary.

2.5.3 The decision of whether or not to release will involve balancing the Data Subject's fundamental right of Subject Access with the rights of the 3rd party to confidentiality.

2.5.4 In many cases, 3rd party information can be simply redacted (removed / blanked out) from the information prior to release. Where this is possible, without affecting the substance or meaning of the information, this should be done.

2.5.5 Where redaction is not suitable, the following two step approach should be considered:

Step 1: Has the 3rd party consented to release? If the 3rd party hasn't been asked, considered if it is appropriate to do so.

Step 2: Would it be reasonable in the circumstances to release without 3rd party consent? Consider:

- Any duty of confidentiality owed to the 3rd party
- Any steps taken to try to get the 3rd party's consent
- Whether the 3rd part is capable of giving consent
- Any stated refusal of consent by the 3rd party
- How much of the information is already generally known to the requester?
- What are the circumstances relating to the individual making the request – how important is the information to them?

2.5.6 If it is decided to disclose 3rd party information without consent, a note of the decision, and the rationale for it, must be kept within the record.

Section 2.6: Exemptions

2.6.1 There are a number of exemptions from the duty to provide subject access. Where one of these exemptions applies, it is not necessary to provide the information in response to a SAR. Specific advice on the application of any applicable exemption should be sought from the IMLO / Legal Services as needed.

2.6.2 The most common of these exemptions are:

- Confidential references given by ACC in connection with an individual's education, training or employment (Note – references received by ACC do not have a blanket exemption)

- Information which is publically available

- Information that is held for the purposes of the prevention and detection of crime; the apprehension and prosecution of offenders and the collection of tax of other duties.

- Management information that is held for the purposes of management forecasting or management planning

- Information relating to on-going negotiations with the requester

- Information held for the purposes of carrying out regulatory functions

- Legal advice provided to services by ACC Legal Services, Legal advice received by ACC and information relating to legal proceedings

- Information held for the purposes of journalism, literature and art or research, history and statistics.

Section 2.7: Special Considerations – Education and Social Work records

2.7.1 There are special considerations to be given when a SAR requests release of either Education or Social Work records.

2.7.2 These special exemptions are:

2.7.3.1 Where information in a Social Work record originates from the Scottish Children's Reporters Administration (SCRA), consent from SCRA must be received prior to that information being released.

In order to ensure that the 40 calendar day deadline for response can be achieved, consent from SCRA must be sought as soon as the need for is identified.

If no response is received, or consent is refused, the information originating from SCRA must not be released.

2.7.3.2 If it is determined that releasing personal information may cause harm to the physical or mental health of the requester or any other person (including staff members), and /or prejudice the carrying out of the Social Work Function the information can be exempted.

The professional judgement of staff should be used to determine if this exemption applied. The reasons supporting a decision to withhold the information must be recorded and kept within the relevant file.

Section 2.8: Responding to a SAR

2.8.1 In the response, the requester should be advised that:

- ACC is the Data Controller for the personal information it holds;
- Given a description of the personal information ACC holds, the reasons it is processed and whether it is shared with any other organisations or people
- Whether the personal information is subject to any automatic decision making

- Advised of the source of the personal information (where this is available).

2.8.2 The right of Subject Access is the right to access the information, not necessarily to receive a copy of it. Providing a copy is normally the easiest way of providing subject access but it can be provided in other ways if it would be a more appropriate way to do so.

2.8.3 If there are any particularly complex terms or codes within the information, an explanation of these must be provided in order that the requester is able to understand the information.

2.8.4 Consideration must be given to the most appropriate method of supplying the information to the requester. This will depend on the specific circumstances of the request but options include via secure e-mail (where the requesters -mail address is confirmed); via Recorded Delivery post or via collection by or delivery to the requester. The method selected may depend on the sensitivity and bulk of the information to be supplied.

2.8.5 A copy of the information should be provided, not the original. If any redactions have been made a copy of the redacted response should be kept on file in order that any later queries can be addressed. The copy supplied should be clearly marked as a copy and a note of the information supplied must be kept on file.

Section 2.9: SAR Checklist

The following 10 Step Guide can assist in ensuring that SAR are handled properly by ACC:

STEP ONE: Confirm it is a Subject Access Request;

STEP TWO: Confirm that you have enough information to be sure of the requester's identity;

STEP THREE: Confirm if you need more information from the requester to find what they want;

STEP FOUR: Confirm if you are charging a fee;

STEP FIVE: Confirm if you have the information that the requester wants**;**

STEP SIX: Confirm that the information has not been changed, except for routine amendments, since receiving the request;

STEP SEVEN: Confirm if the information contains personal information about other people and, if it does, confirm how this will be managed;

STEP EIGHT: Confirm if any exemptions apply which would stop the information being released;

STEP NINE: Confirm if any explanation is necessary for any complex terms or codes contained in the information;

STEP TEN: Prepare the response.

APPENDIX FOUR - CORPORATE ACCESS TO PERSONAL INFORMATION (THIRD PARTY) PROCEDURE

Protection Procedure – Access to Personal Information (Third Party Access)

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1.0	15th September 2015	-	Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1. Introduction

1.1 The purpose of this procedure is to outline the way in which requests from parties other than the data subject which are received by Aberdeen City Council (ACC) should be handled.

1.2 The way in which requests for access to personal information are handled depends on who makes the request and care should be taken to ensure that the correct procedure is followed.

- Where a request is received from the data subject (the person about who the information relates) or from someone acting on the data subjects behalf, the request is a **Subject Access Request** (See Subject Access Request procedure).
- Where a request is received from a person other than the data subject or his representative or from another organisation / agency, the request should be handled as a **Third Party Request for Personal Information** (See Section 2).

2. Third Party Request for Access to Personal Information

Section 2.1: Introduction

2.1.1 Occasionally access to the personal information held by ACC is requested by external persons and organisations. There are a number of specific circumstances in which such requests will be agreed, namely:

- Requests from other ACC Services (See Section 3.2)
- Requests from Elected Representatives (Councillors, MSP's, MP's & MEP's) (See Section 3.3)
- Requests from Government Agencies (See Section 3.4)
- Requests from Parents (See Section 3.5)
- Requests from the Police (See Section 3.6)
- Requests from Solicitors and Courts (See Section 3.7)
- Requests from Schools (See Section 3.8)

If a request falls within one of these categories then the procedure highlighted in the relevant section below must be followed.

2.1.2 In all other circumstances, prior to agreeing any request, consideration must be giving to the knowledge of the data subject and whether the data subject has consented to the release.

2.1.2.1 If the data subject is aware of the possible transfer of personal information to a 3rd party and has consented to it, then the information can be released in response to the request. A note of the request, of the awareness and consent of the data subject, and of what information was released should be made and stored in the file.

3.1.2.2 If the data subject has not consented to the release of their personal information to a 3rd party then to do so would likely breach the Data Protection Act 1998 and the Human Rights Act 1998. Legal Advice

must be sought prior to releasing personal information in response to such a 3rd party request where consent of the data subject has not been received.

Section 2.2: Requests from other ACC Services

2.2.1 Personal information held by ACC is held for a specific purpose or purposes and, if a service wishes to access personal information held for a different purpose (eg: Social Work requesting access to information held for the purpose of processing an application for housing), the following procedure must be followed.

2.2.2 In respect of one-off requests for the sharing of specific information:

2.2.2.1 If the data subject is aware of the possible sharing of personal information with another service and has consented to it, then the information can be released in response to the request. A note of the request, of the awareness and consent of the data subject, and of what information was released should be made and stored in the file.

2.1.2.2 If the data subject has not consented to the release of their personal information to another service, then consent can be sought. If no consent is given, sharing the personal information across services would likely breach the Data Protection Act 1998 and the Human Rights Act 1998.

2.2.3 In respect of routine transfers of personal information, for example Council Tax information, data subjects must, at the point of collection, be advised, via a Privacy Notice, of all of the purposes for which the information will be used by ACC.

2.2.4 If a proposed routine transfer is planned after the time when the personal information was collected, the data subject should be advised of the planned new purpose and given the opportunity to

object to this processing or be asked to provide consent to it being done.

2.2.5 Council Tax information can been used by ACC for purposes other than Council Tax processing so long as there is a legitimate reason for doing so and that use in the way proposed will not result in genuine unfairness or unwarranted detriment to the data subject.

2.2.6 The ACC Internal Audit function prepares an Annual Plan which details the audits to be undertaken each year. Internal Audit is a legitimate management function of ACC therefore the Internal Audit provider can, where authorised to do so, access information maintained by ACC, including personal information. However, this does not mean that Internal Audit staff can have unlimited access to all documents and files containing personal information. Data Protection requirements must be adhered to and, where relevant, the consent of the data subject to release must be sought.

2.2.7 From time to time personal information will require to be disclosed to ACC's insurance provider in order to process an insurance claim or defend a legal action. However, this does not mean that the Insurance Provider can have unlimited access to all documents and files containing personal information. Data Protection requirements must be adhered to and, where relevant, the consent of the data subject to release must be sought.

Section 2.3: Requested from Elected Representatives

2.3.1 Whether or not a member of staff can disclose personal information/data to an Elected Member is dependent upon the role the Elected Member is fulfilling at a particular time. Elected Members may fill one of three roles:

- They may act as a member of Aberdeen City Council (ACC), for instance as a member of a Committee (i.e. official council work).

  - Disclosures of personal data may be made to an Elected Member, if it is necessary for him/her to carry out official duties. When disclosing personal data to an Elected Member, staff must specify the purposes for which that information may be used or disclosed.

- They may act as a representative of residents who live in their ward, for instance, in pursuing complaints (i.e. constituency work).

  - Personal data may always be disclosed at the request of or with the consent of an individual. The consent of the individual concerned is not normally required, provided that the Elected Representative represents the ward in which the data subject lives and there is a reasonable presumption that the Elected Member/ MP or MSP is acting on behalf of the individual.
  - Where sensitive personal data is to be disclosed to an Elected Representative, the Information Commissioner advises that it is prudent to obtain the written consent of the data subject.

- They may represent a political party, particularly at election time.

  - Personal information will not normally be disclosed to Elected Representative for political purposes unless the data subject has given written consent to this being done.

Section 2.4: Requests from Government Agencies

2.4.1 Personal Information may be requested by Government Agencies for many purposes. ACC encourages a co-operative and responsible working relationship with Government Agencies and Regulatory Bodies. In order to achieve this ACC will normally share personal information in the interests of multi-agency working and provide specific personal information where requested, where it is lawful to do so.

2.4.2 National Fraud Initiative

The National Fraud Initiative in Scotland is a counter-fraud exercise led by Audit Scotland, assisted by the Audit Commission (its sister organisation in England). Certain categories of information are requested annually from ACC by Audit Scotland as part of the National Fraud Initiative. The information requested must be provided within the specified time-frame (in accordance with the terms of the Local Government (Scotland) Act 1973).

ACC requires to ensure that individuals are informed that their information may be disclosed for the purposes of auditing in order to identify possible fraud. Individuals should, wherever possible, be informed of this prior to the disclosure taking place. It should be noted that individuals are only required to be informed of the disclosure – not given the opportunity to consent or object to it.

2.4.2 Circumstances where Information can be disclosed to a Government Agency or Regulatory Body

2.4.2.1 It is always lawful to disclose information to any Government Agency or Regulatory Body where the individual concerned is aware that their information may be disclosed to that Government Agency or

Regulatory Body and has consented to this being undertaken.

2.4.2.2 Information can be disclosed without the consent of the individual concerned where this is necessary for:-

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of any tax or duty or of any imposition of a similar nature

Each request for disclosure under these categories must provide you with enough information to enable you to be satisfied that it is necessary to disclose the information which has been requested, e.g that information is required for benefit fraud reasons and that ACC has up to date information held by its Revenues section which HMRC does not have access to. Furthermore, if the information is required for one of the purposes outlined above then the individual concerned will not require to be told of the disclosure. This is because the investigation may be prejudiced if the individual found out about it.

2.4.2.3 Many Government Agencies and Regulatory Bodies have extensive Statutory Powers which enable them to obtain personal information and ACC can provide the information sought under a specific exemption in the Data Protection Act. If they are acting under such powers then this should be made clear within the request letter. If there is any doubt as to why

information is sought or as to in what capacity the Agency/Body is acting then clarification should be sought.

Section 2.5: Requests from Parents

2.5.1 Parents (with parental rights and responsibilities) and guardians of children under the age of 12 can exercise the child's right of access on the child's behalf. Any such request should be processed as a SAR.

2.5.2 Once a child is over the age of 12 they are deemed to capable of making their own decisions with regards to their personal data. As such, parents generally lose the right to access the child's personal information without the consent of the child.

2.5.3 An exemption to this general principle is parents' rights of access to their child's educational record. Such requests should be handled as follows:

2.5.3.1 The Pupil's Educational Records (Scotland) Regulations 2003 ("the Regulations") set up a framework for the disclosure of a pupil's educational records to a parent. The regulations define "*educational records*" as any records of information, excluding information contained in a Record of Needs or a Co-ordinated Support Plan, which-

(a) are processed by or on behalf of the Education Authority;

(b) relate to any person who is or has been a pupil at the school;

(c) relate to the school education of that person; and

(d) originated from or was supplied by either:

(i) a teacher;

(ii) any other employee of the Education Authority;

(iii) the pupil to whom the information relates; or

(iv) a parent of that pupil.

2.5.3.2 Essentially, the Regulations state that, upon receiving a request by a parent for disclosure of their child's educational record, the Education Authority/School must, within 15 school days either:

- make the educational record available, free of charge, for inspection by the parent; or
- provide a copy of the educational record to the parent, subject to the payment of such fee as the School/Education Authority think fit, up to a maximum of £50.00

Section 2.6: Requests from the Police

2.6.1 It is always lawful to disclose information to the Police where the individual concerned is aware that their information may be disclosed to the Police and has consented to this being undertaken. Consent could be gained by, for example, signature of a form incorporating a full explanatory data protection statement.

2.6.2 Information can be disclosed to the Police without the consent of the individual concerned where this is required for the purposes of safeguarding national security. This section could be utilised, for example, in the event of a suspected terrorist attack.

2.6.3 Information can also be disclosed to the Police without the consent of the individual concerned where this is required for:-

- the prevention or detection of crime;
- the apprehension or prosecution of offenders;
- the assessment or collection of any tax or duty or of any imposition of a similar nature

2.6.4 This information can be released because there are specific exemptions with the Data Protection Act 1998 covering these situations. ACC does not have to agree to any request from the Police, and will only do so if it is satisfied that it is necessary to release the requested information to the Police.

2.6.5 If information is released to the police for the purposes outlines in 2.6.2 and 2.6.3 then the data subject concerned will not require to be told of the disclosure. This is because the investigation of the crime may be prejudiced if the individual found out about the investigation.

2.6.6 Information can also be disclosed to the Police without the consent of the individual concerned where this is necessary in order to protect the vital interests of any person. This means where a person is faced with a life/death situation in which the Police must intervene. In this type of situation, Staff should still ensure that the information provided on an urgent basis in such a situation is provided in accordance with paragraph 3 below.

2.6.7 <u>Procedure for dealing with a Request from the Police</u>

2.6.7.1 All requests must be received in writing and contain:

- Details of the purpose for which the Police require the information and a brief explanation of why they believe the information is required by them.
- a description of the information required.
- details of the Rank, Number and Name of the Police Officer requesting the information, the Police Station where that Police Officer is situated and the main office telephone number and extension number for that officer, or the Head Office address and contact details for that particular Police Authority.
- A copy of the data subject's consent, or confirmation that explicit consent from the data subject has been obtained and a note of any concerns/ wishes or restrictions of the consent where this is appropriate.

1.6.7.1 If all of the information listed is not included in the request, then the Police must be contacted and asked to provide all of the relevant information prior to the information being disclosed.

1.6.7.2 On receipt of all of the above information the request can be fully responded to. Only copies of the information specifically requested can be disclosed. You should mark the information clearly as a "COPY" so that it is clear it's not the original. Details of the information disclosed, the date and the method of disclosure should be noted in the relevant file. The individual who is the subject of the information does not require to be told of the disclosure.

1.6.7.3 When disclosing the information requested, it must not be faxed to a Police Force, even if they request you to. Ensure you have either sent the information via a secure email, such

as gcsx, gsi or pnn etc, or have password protected it using Mircosoft Office 2010.

Section 2.7: Requests from Solicitors and Courts

2.7.1 Requests from Solicitors and Courts will broadly fall under three categories, as follows:

2.7.1.1 A Court Order requiring ACC to release Personal Information

Any court can order that ACC release personal information if that specific information is required in order to proceed with a civil or legal case.

Where such a Court Order is received it must be adhered to.

The Court Order will contain details of the specific information which is to be released and state the time limit by which the information is to be provided. The information must be supplied by the deadline specified.

Care must be taken to ensure that only the information requested is provided. In some circumstances, redaction of information other than that required may be necessary.

2.7.1.2 A request from a Solicitor acting on behalf of the Data Subject

A request made by a Solicitor representing the Data Subject should be treated as a Subject Access Request.

2.7.1.3 A request from a Solicitor acting on behalf of a 3rd Party

ACC is not obliged to disclose personal information sought by a Solicitor acting for a 3rd Party. Any such request should be considered carefully and, if release is not justified, the Solicitor should be advised it is refused. ACC can stipulate that it prefers to await the receipt of a court order requiring release.

Section 2.8: Requests from Schools (Transfer of Pupil Records)

2.8.1 Where a pupil transfers to another school, which is also an Aberdeen City Council (ACC) school then that pupil's original record should transfer automatically to the new ACC school. The original record may be transferred – a copy does not have to be retained by the sending school.

2.8.2 When dealing with a request from a new school that is within the UK, but is not an Aberdeen City Council school, a copy should be made of the pupil's entire educational record including sensitive personal data. The copy should be clearly marked as a "COPY".

Any information which could identify a third party i.e. anyone other than a teacher, an employee of the education authority, the pupil themselves or the pupil's parent (this could include, for example, mention of another pupil, another pupil's parent, or a named police officer) should be redacted or removed from the information being sent.

The copy of the record, excluding any third party information, should be sent to the new school as soon as possible and in any case within 15 school days.

The information should be sent by first class recorded post or electronically via a secure email address or password protected.

The original Record of Needs or Co-ordinated Support Plan, if there is one, should also be transferred to the new school or Education Authority. The original educational record and a copy of the Record of Needs or Co-ordinated Support Plan should remain within the school archives.

2. <u>Sources of Further Information and Advice</u>

The Data Protection pages on the Zone contain links to a number of ICO publications which can provide further information on Accessing Personal Information.

Advice on responding to any request for access to personal information is available in the first instance from the appropriate Service IMLO. Team 2, Commercial & Advice Team, Legal Services can provide IMLO's with specialised advice on request.

APPENDIX FIVE - CORPORATE SHARING PERSONAL INFORMATION PROCEDURE

Corporate Data Protection Procedure – Sharing Personal Information

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1.0	15th September 2015	-	Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1.0 Introduction

1.1 On occasion Aberdeen City Council (ACC) may require to pass personal data to an external agency for processing[1] on ACC's behalf. In that case this procedure must be followed.

1.2 Please note that if information is being routinely shared with an external agency for that agency's own use then the Corporate Data Protection Procedure entitled "Routine Data Sharing Procedure" should be adhered to.

2.0 Compliance with Standing Orders and Financial Regulations

2.1 If ACC is entering into any contract with an external agency to carry out data processing then on its behalf, as with any other contract, compliance with ACC Standing Orders and Financial Regulations is required.

[1] "Processing" includes obtaining; recording or holding; disclosing by transmission, dissemination or otherwise making available; organising, adapting or altering; retrieval, consultation or use of the data; alignment, combination, blocking, erasure or destruction of the data.

3.0 Consultation with other Services

3.1 Where personal or sensitive personal information is to be processed by an external agency, the Service must consider at the outset the following:

1. What technical measures/ safeguards should be put in place to ensure the data remains secure (e.g. compliance with BS ISO/IEC 270001 on information governance and BS779-3 on information security risk management or other equivalent; whether the system is a hosted system; if a website or webpage is to be used, whether this meets the Web Content Accessibility Guidelines and is cookie compliant and access protocols in relation to any personal information processed.
2. When to consult with staff in ICT, HR and Legal Services to ensure that the contractual documentation contains clear expectations around the use of data during the contract and after.
3. How the data will be transferred to the external agency, e.g requirements for it to be protected in transit whether the transfer is electronic or physical, and
4. What additional measures, if any, are required.

4.0 Data Processing Agreements

4.1 If any agreement is to be entered into whereby personal or sensitive personal data is to be transferred to any external agency for processing then the Head of Legal and Democratic Services shall be informed prior to that agreement being signed by the Council.

4.2 A legally binding separate Data Processing Agreement shall be entered into, or a robust Data Processing section shall be included in the body of the larger contract, as appropriate.

5. Further Information

5.1 If you require further information or have any queries contact the Information Management Liaison Officer (IMLO) for your Service. Details of the IMLOs can be found on the Zone.

APPENDIX SIX - CORPORATE DATA PROTECTION INCIDENTS PROCEDURE

Corporate Data Protection Procedure – Reporting of Data Protection Incidents

Document Control

Version	Date Approved	Page(s) Amended	Approved By
v.1	15th September 2015	-	Fiona Smith, Corporate Governance. Finance, Policy & Resources Committee

Contents

1. Introduction

1.1 The purpose of this procedure is to ensure that the same approach is taken throughout Aberdeen City Council (ACC) in relation to the reporting and management of a data protection incident under the Data Protection Act 1998 (DPA). The Corporate Data Protection Policy sets out ACC's legal obligations under the DPA and the common standards all staff and Elected Members must comply with in order to comply with the eight Data Protection principles.

1.2 ACC takes any incident which does, or may lead to a, breach of the DPA seriously. Depending on the particular circumstances of the breach, the Corporate Policy provides that such may attract disciplinary proceedings against that member of staff.

1.3 There are two types of Data Protection incident which this procedure requires are reported, Data Protection breaches and Data Protection Near Misses.

2. Data Protection Breaches

2.1 What is a Breach?

2.1.1 The DPA requires ACC to comply with the eight data protection principles contained within the Act. A breach is a failure to comply with any of these principles. The following list, which is not exhaustive, provides examples of what is considered a breach of the Corporate Policy and Procedures which would require to be reported under this procedure:

- the unauthorised access and/ or use of personal (or sensitive personal)[1] information by a member of staff[2] or elected Member;
- unauthorised disclosure of personal (or sensitive personal) information;
- accidental loss;
- theft of personal (or sensitive personal) information;
- failure to process personal (or sensitive personal) information appropriately in accordance with the principles;
- failure to adhere to the Corporate Policy and/ or Procedures and other relevant procedures in relation to the processing of personal (or sensitive personal) information;
- failure to destroy or retain records or personal (or sensitive personal) information appropriately in accordance with legislation or council policies/ procedure;
- human error which results in any of the above having occurred;

[1] Sensitive personal information is information consisting of information as to; racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of an offence or any proceedings for any offence committed or alleged to have been committed or the disposal of any such proceedings or the sentence of any court.

[2] The term "Staff" includes full time, part time, temporary and contract employees.

- using personal (or sensitive personal) information for a purpose which is incompatible with the consent obtained or legitimising condition e.g. providing social work information to Housing, for a housing related matter where consent has not been provided and there is no requirement to share that information under any statutory power.

It should be noted that a breach of the Corporate Policy or Procedures may also be deemed a breach of the ICT Acceptable Use Policy and the ICT Good Practice Guidelines.

2.2 Notification of Breaches

2.2.1 All breaches must be reported to the Business Manager or Directorate Support Manager immediately, or within 2 working days of the breach being discovered. A breach must be reported immediately where the information is considered sensitive personal information and/ or the breach is likely to cause a risk to service users or others.

2.2.2 The Business Manager or Directorate Support Manager must notify the Director of the breach upon hearing about it, if the breach requires immediate reporting. Notification can be by telephone or by email. Thereafter, the Director (or a representative acting on their behalf in their absence) shall inform the Head of Legal and Democratic Services of the breach the same day.

2.2.3 Within 2 working days of the breach occurring or having been made known, the line manager must complete the Reporting Form at Appendix A and forward it to the Business Manager or Directorate Support Manager.

2.2.4 Upon receiving the Reporting Form, the Business Manager or Directorate Support Manager shall forward the Reporting Form to the Director and Head of Legal and Democratic Services, who is responsible for maintaining the breach register.

2.2.5 Depending on the circumstances and nature of the breach it may be necessary to report the breach to the Information Commissioner. The Head of Legal and Democratic Service is responsible for reporting matters to the Information Commissioner.

2.2.6 The Head of Legal and Democratic Services shall report to the Corporate Management Team on a biannual basis, or with such frequency as is deemed appropriate, on any areas which require further action which arise from any breaches reported to her.

2.3 **Assessing the risks**

2.3.1 Before deciding what steps are necessary further to immediate containment, the risks associated with the breach must be fully considered. One important consideration is an assessment of the potential impact on the individual(s) and what the consequences are for that individual or any other relevant parties, including ACC.

2.3.2 In assessing the impact of a risk, the following points should be considered:

- What type of information is involved?
- How sensitive is it? Some information is sensitive because of its very personal nature.
- How was the information held, e.g. (a file, on a USB stick, in an email).
- Who had, or has had access to the information? (were they authorised to have access)?

- If information/data has been lost or stolen, is it protected? Is the information encrypted? Has a call been logged with the IT helpdesk to report the loss or theft of any ICT resource (e.g. USB stick, laptop, RAS token, smart phone, mobile phone).
- What could the information/data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?
- Who are the individuals whose data has been breached? Whether they are staff, service users, or contractors will to some extent determine the level of risk posed by the breach. Determining who the individual(s) are will inform the action to be taken to mitigate the risks.
- What harm can come to those individuals? E.g. Physical safety, distress, reputation, financial loss, other aspects of life.
- Are there wider consequences to consider? Such as loss of public confidence, press interest?
- Should the breach be reported to the Police?

2.4 Investigation and Recovery

2.4.1 The Business Manager or Directorate Support Manager must decide within their service who should take the lead on investigating the breach. This may involve discussion with HR, IT, Legal services, and where appropriate, the Police.

2.4.2 The Business Manager, the Directorate Support Manager or Investigating Officer must establish who needs to be made aware of the breach and need to establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.

2.4.3 Having considered the risks detailed in clause 2.3 above, the investigation needs to establish how the breach occurred, why it

occurred, what was steps should be put in place to prevent the breach happening again in the future.

2.4.4 The outcome of the investigation should be recorded in the Reporting Form. If the Reporting Form has already been submitted prior to the investigation, it should be updated.

2.4.5 The updated Reporting Form should be sent to the Business Manager or Directorate Support Manager within two weeks of the breach having occurred or becoming known. The Business Manager or Directorate Support Manager should, upon receipt of the updated Reporting Form, send it to the Director and Head of Legal and Democratic Services.

2.5 Informing Service Users and Others

2.5.1 Informing service users and others about a breach is an important element of managing breaches. Notification should have a clear purpose, whether this is to enable service users who may be affected to take the necessary steps to protect themselves or to allow the appropriate bodies to perform their functions.

2.5.2 The following questions may assist you in deciding whether to notify:

- Can notification help the individual/service user? Not every breach will warrant notification.
- Will notification by detrimental to the individual/service user?
- Are the consequences of the breach of a serious nature?
- Consider how notification should be made, for example if you are notifying vulnerable individuals, or children.

2.5.3 The line manager must assess the risk and decide on the appropriate action to be taken. The proposed action should be clearly detailed in the Reporting Form.

2.5.4 Line managers should consider how notification should be made. This will depend on the situation. There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium which was used as well as the urgency of the situation.

2.5.5 Notification should at the very least include a description of how and when the breach occurred and details of the personal (or sensitive personal) information.

2.5.6 It may be considered appropriate to notify individuals by telephone, personal visit, or letter. Particular care should be taken when considering the most appropriate method for particular groups of individuals, for example, if you are notifying children or vulnerable adults, it may be appropriate for a representative to be present.

2.5.7 When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.

2.5.8 Provide a way in which they can contact you for further information or to ask you questions about what has occurred. You should also provide them with information on how they can make a formal complaint to the Council or the Information Commissioner's Office. Complaints made to the Information Commissioner's Office should be made in writing to First Contact Team, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF, or by email to casework@ico.gsi.gov.uk

3. Data Protection Near Misses

3.1 What is a Near Miss?

3.1.1 A Near Miss is defined as an unplanned occurrence which did not ultimately lead to a data protection breach taking place but had the potential to. Such an occurrence may be the near sending of an e-

mail or letter to the wrong recipient or the near loss or inappropriate sharing of personal information.

3.1.2 The importance of recording and reporting near misses is to assist with the identification of any inherent system or process weaknesses which could, unless addressed, lead to a Data Protection breach occurring.

3.2 Notification of Near Misses

3.2.1 An identified near miss should be reported to the Business Manager or Directorate Support Manager within 5 working days of it occurring by completing the Near Miss Reporting Form.

3.2.2 Upon receiving the Reporting Form, the Business Manager or Directorate Support Manager shall forward the Reporting Form to Team 2 in Commercial & Advice, Legal Services who are responsible for maintaining a register of near misses.

3.2.3 Any trends or patterns in reported near misses will be identified by the Commercial & Advice Team or Business Manager and any system or process weaknesses which are addresses will be highlighted to the appropriate officer.

4. Advice and Guidance for Staff

4.1 For further Data Protection advice or guidance staff should contact the Information Management Liaison Officer for the service, details of which can be found on the Zone.

Ref Number:

APPENDIX 1- CORPORATE REPORTING FORM

Reporting Officer Name:	✉ ☎
Business Manager/ Directorate Support Manager:	✉ ☎
How was the breach discovered (include the date of the breach)?	
How would you categorise the breach (*please tick where applicable)* **Loss** ☐ **Theft** ☐ **Unauthorised Disclosure** ☐ **Unauthorised Access** ☐ **Human Error** ☐ **Unauthorised Use** ☐	
What information was involved and who did it relate to?	
How was the information held (e.g. online, on a laptop, contained within an email).	
Explain the consequences of the breach (include information about who has had access to it and/ or what the potential affect the breach may have on the person the information is about, press interest).	

Provide a description of the immediate measures taken to mitigate the impact of the breach.	
Explain what proposed measures/ actions you intend to put in place to prevent the breach occurring in the future.	
When was the breach reported to the Business Manager or Directorate Support Manager?	
When was the breach reported to the Director?	
Has an internal investigation been ordered?	Yes ☐ No ☐
If yes, please advise who will be undertaking the investigation	
When will it be completed by:	

Forward the completed proforma to the Business Manager or Directorate Support Manager within 2 working days of the breach.

For Admin use only

Update required? Yes ☐ No ☐	Deadline (date)	Advise Director of date update required ☐
Reported to Head of Legal and Democratic:	Update form on register ☐	