INFORMATION MANAGEMENT

Prepared by:	Rochford District Council
Author:	SIRO
Date:	February 2022
Version:	8

1. Introduction

Information resources are vital to the Council in the delivery of services to residents, business and visitors. Their availability, integrity, security and confidentiality are essential to maintaining service levels, legal compliance and the public image and perception of the Council.

The Council is the Data Controller and it has a responsibility to ensure appropriate and proportionate security of the personal data they hold. This is covered by the 6th principle of the GDPR as detailed below:

> *"*Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')"

It is important that residents are able to trust the Council to act appropriately when obtaining and holding information and when using Council facilities. It is also important that information owned by other organisations made available to the Council under secondary disclosure agreements is treated by the Council with the same level of security.

Any public authority that uses or provides information resources has a responsibility to maintain and safeguard it and to comply with the laws governing the processing and use of information and communications technology.

The Council's Leadership Team has ultimate responsibility for the management of information and endorses the adoption and implementation of this document and the procedures within it.

- Appendix A sets out the Information Asset Owners and their Deputies
- Appendix B set out the procedure in how to deal with data breaches.
- Appendix C contains the data security breach risk assessment form.

This procedure note has been designed to provide guidance on the appropriate level of protection against misuse of information and to prevent unauthorised disclosure of information for which the Council is responsible. It lays down clear standards of practice required of Council employees and partners when handling sensitive or confidential information. Supporting this document is a set of information management policies, guides and procedures which form the minimum standards with which partners must comply. Individual organisations may strengthen these through local policies and procedures, but cannot weaken them. In addition, users who are granted access to information owned by other organisations will be subject to the policy requirements of the information owners, the detail of which must be provided before access is granted.

It is unacceptable for the Council's information resources to be used to perform unethical or unlawful acts.

The key elements of this and all associated policies have been developed in accordance with the British Standard for Information Security BS7799 – 3:2006 which is harmonised with ISO/IEC 27001:2005.

2. The Law

THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

Under GDPR everyone responsible for using data has to follow six strict rules called the GDPR principles. You must make sure the information is:

1. Processed lawfully, fairly and in a transparent manner (must have legitimate grounds for collecting the information; be transparent about how you are going to use it and explain this in Privacy Notices when it is collected)

2. Collected for specified, explicit and legitimate purposes (it must be clear from the outset about why you are collecting personal data and what you intend to do with it)

3. Adequate, relevant and limited to what is necessary (you should only collect the minimum amount of data needed)

4. Accurate and, where necessary, kept up to date

5. Retained only for as long as necessary (information should not be kept longer than the appropriate time period in the Council's Document Retention Policy)

6. Processed in an appropriate manner to maintain security (the security of the data you have collected must be considered at all times)

Data Protection covers all 'personal information' relating to living individuals that is held either on computer systems or manual filing systems. It is a criminal offence to hold or disclose information in breach of the requirements of the Data Protection Act.

It applies to anyone who handles or has access to information about individuals. It also gives rights to people who are the data subject to enable them to find out what personal information the Council holds about them.

The Freedom of Information Act 2000 (FOIA)

The FOIA gives a general right of access to all types of data and information that has been recorded by the Council. There are exemptions to the right of access, but the Council must assist applications for information and proactively make details available. The Council must know what records it holds, where they are stored and must avoid them being lost.

The Computer Misuse Act 1990 (CMA)

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and would constitute an offence under the CMA for which the penalties are imprisonment and/or a fine.

The Companies Act 1985 (CA)

The CA requires that adequate precautions are taken against the falsification of records and to the discovery of any falsification that occurs.

The Human Rights Act 1998 (HRA)

Public authorities must consider the implications of the European Convention on Human Rights, in particular Article 8: the right to respect for private and family life, when storing and processing personal information.

The Regulation of Investigatory Powers Act 2000 (RIPA) The RIPA framework and legislation regulates advances in technology and surveillance capability and recognises individuals' rights as set out in the HRA in the use of covert investigations by a number of bodies, including local authorities.

Please contact the Council's Legal Services department to discuss the provisions of the above legislation in more detail.

3. Legal and regulatory obligations

The Council will comply with all relevant legislation affecting the use of information and communication technology. All users must be made aware of and comply with current legislation as they may be held personally responsible for any breach.

4. Scope and application

This guidance applies to the creation, acquisition, retention, transit, use and disposal of all forms of information.

It applies to all employees and elected Members; agency workers; volunteers; work experience candidates and all staff of service delivery partners and other agencies who handle information for which the Council is responsible. It will form the basis of contractual responsibilities as set out in mandatory contract clauses where reference is made to this toolkit.

5. Objectives

The Council's information management objectives are:

- All users are aware of the Council's policies and procedures in relation to information management.

- All users are aware of the legal and regulatory requirements and of their responsibilities in relation to information management.
- All Council property, including equipment and information, is appropriately protected.
- The availability, integrity and confidentiality of Council information is maintained.
- A high level of awareness exists of the need to comply with information management measures.
- Unauthorised access to software and information is prevented.
- The risk of the misuse of email is reduced.
- The network and network resources are protected from unauthorised access.
- Guidance is provided on handling information of each classification in different circumstances and locations including creation; modification or processing; storage; communication; retention and deletion and disposal or destruction.
- Unwanted incidents, such as virus infections, deliberate intrusion and attempted information theft, are managed.
- Unauthorised access, damage and interference to business premises, information and information technology is prevented.

6. Council policies, guides and procedures

All individuals, corporations and others to which this document applies (see paragraph 4 above) must be aware of and adhere to the following Council policies and procedures in relation to information management:-

- Conditions of acceptable use and personal commitment statement
- Data Protection Policy
- Records and retention management
- Subject Access Request
- Clear desk policy and procedure
- Guide to e-mail management
- Procedure for gaining access to other staff's e-mails
- Procedure for reporting information security incidents
- Procedure for taking data outside the work place
- Procedure for the installation of software
- Procedure for using RDC equipment outside the work place
- ICT policies disciplinary procedures

7. People and their Roles

Managing Director and Strategic Director

The Managing Director and the Strategic Director are ultimately responsible for ensuring that all information is appropriately protected.

Leadership Team

The Council's Leadership Team is responsible for the review and approval of this document and the policies, guides and procedures listed in paragraph 6 above, which are reviewed and re-issued each year. The team is also responsible for approving and overseeing all information security related projects and initiatives.

Senior Information Risk Owner (SIRO)

The Council must appoint a Senior Information Risk Owner (SIRO) to ensure there is accountability. At present, the Council's SIRO is the Council's Section 151 Officer – Naomi Lucas (naomi.lucas@rochford.gov.uk)

The SIRO must provide written judgment of the security and use of the business assets at least annually to support the audit process and provide advice to the accounting officer on the content of their statement of internal control.

The role of the SIRO includes:

- Taking the lead on overseeing information risk management and security in the Council and assisting the Leadership Team in the delivery of this.
- Providing support where appropriate to the Data Protection Officer in all aspects of information security.
- oversee the information security function
- oversee incident management and risk management
- oversee security management and reporting
- Providing advice on government and best practice security standards and practices to help combat security threats.

It is not concerned solely with IT, but takes a broader view of the Council's information assets as a whole, in any form.

Data Protection Officer (DPO)

The Council must appoint a Data Protection Officer under the new GDPR regulations to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed.

The DPO for the Council is the Assistant Director, Legal & Democratic Services - Angela Law (DPO@Rochford.gov.uk)

Information Asset Owners and Deputies

Each Assistant Director is an Information Asset Owner (IAO) unless the role has been delegated to a deputy and this person. The IAO will understand what information is held within their department, how it is used and transferred and who has access to it and why. The IAOs and their deputies are listed in Appendix A.

The IAOs are tasked with ensuring that the best use is made of information and receiving and responding to requests for access.
They are responsible for:-

- Assessing the risks to the information and data for which they are responsible in accordance with the Council's Corporate Risk Management Framework and Policy, which sets out the strategy for managing risk together with the assigned roles and responsibilities;
- Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information;
- Defining the value of information, and identifying the risks associated with it. Information must be classified and controls defined for its protection.
- Ensuring that their staff are fully conversant with this guidance and all associated policies, guides and procedures and relevant legislation, and are aware of the consequences of non-compliance;
- Developing procedures, processes and practices which comply with this document for use in their individual business areas;
- Ensuring that all external agents and third parties defined in the scope of this document are aware of their requirement to comply;
- Ensuring that, when requesting or authorising access for their staff, they comply with the standards and procedures defined by the Information Owners;
- Notifying the Data Protection Officer of any suspected or actual breaches or perceived weaknesses of information security.

Officers

Council officers are responsible for:-

- Ensuring that their business is conducted in accordance with this guidance and all applicable supporting policies.
- Familiarising themselves with this guidance and all applicable supporting policies, guides and procedures. It is important that they are aware of their responsibilities to keep information secure and not disclosing it without proper cause.
- Only accessing systems and information, including reports and paper documents, to which they are authorised;
- Using systems and information only for the purposes for which they have been authorised.
- Complying with all applicable legislation and regulations.
- Complying with the controls defined by the Information Owner.

- Complying with all the policies and requirements of other organisations when granted access to their information.
- Not disclosing confidential or sensitive information to anyone without the permission of the IAO or their deputy, and ensuring that sensitive information is protected from view by unauthorised individuals.
- Keeping their passwords secret, and not allowing anyone else to use their account to gain access to any system or information.
- Notifying their line manager or the Data Protection Officer of any actual or suspected breach of information security, or of any perceived weakness in the organisation's Security Policies, Procedures, Practices, Process or infrastructure in accordance with the Appendix B below in this document ("Dealing with a breach").
- Protecting information from unauthorised access, disclosure, modification, destruction or interference.
- Not attempting to disable or bypass any security features which have been implemented.
- Reporting any actual or suspected information security incidents or problems and assisting with their resolution.

Officers are also responsible for the management of third parties and must ensure that the third parties are contractually obliged to comply with this document. In the event of a potential breach, the officer must notify the Data Protection Officer.

8. Data Security Breaches

Data security breaches can happen for a number of reasons including:-

- Loss or theft of data or equipment on which data is stored.
- Loss or theft of hard copy documents/files
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.
- A hacking attack.
- Information obtained by surreptitious or deceptive means (blagging)
- Information being released inappropriately

Appendix B provides the procedure and guidance where an incident has occurred. It is imperative that staff act quickly and notify their line manager or IAO or DPO as soon as there has been a data breach.

Breaches can be categorised according to the following three information security principles:-

- 'Confidentiality breach' - where there is an authorised or accidental disclosure of, or access to, personal data.

- ‘Availability breach’ – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- ‘Integrity breach’ – where there is an unauthorised or accidental alteration of personal data.

The Council is under an obligation to report some breaches of data security to the Information Commissioner Office (ICO), especially if a large number of people are affected or there are very serious consequences arising from the security breach. In the case of a personal data breach the Council shall without undue delay and where feasible, inform the ICO no later than 72 hours after having become aware.

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job, for example, where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the Council.

Whilst this type of incident can still have significant consequences, the risks are very different from those posed by, for example, theft of a customer database, the data on which may be used to commit identity fraud.

APPENDIX A

DIRECTORATE	INFORMATION ASSET OWNER	DEPUTY
Chief Executive	Jonathan Stephenson	Angela Hutchings
Legal & Democratic	Angela Law	Julie O'Brien George Sullivan Lauren Quigley Sonia Worthington Chris Irwin
Resources	Naomi Lucas	Emma Turner Kate O'Brien Pam Shepherd Carrie Cox
Assets & Commercial	Matt Harwood White	Mark Aldous Darren McLoughlin Jeff Stacey Rob French Sharon Braney
People & Communities	Louisa Moss	Andrew Paddon Jeanette Hurrell Steven Greener Andy Parkman
Place & Environment	Marcus Hotten	Vanessa Conroy Adam Aldridge Richard Snape Yvonne Dunn Mike Stranks Katie Rodgers / Claire Buckley Daniel Goodman
Transformation & Customer	Dawn Tribe	Sarah Orchard Val Grimwade Ami Goulter Luke Mackenzie

APPENDIX B

Dealing with a breach

Depending on the seriousness and impact of the security breach the DPO may set up a meeting, including the Information Asset Owner, to consider the following:-

- Communication and who needs to be informed within the Council.
- Containment to limit the damage and recovery of any data lost.
- Producing an assessment of the ongoing risk to data subjects.
- Notification of the breach to the Information Commissioner
- Evaluating current practices and the Councils response to the breach.

As soon as a breach has been identified the officer must immediately report the incident to their Information Asset Owner or the Data Protection Officer.

In order to assess the risks following a data security breach and, in helping to determine what steps are necessary following immediate containment, the Officer and Information Asset Owner should complete the Data Security Breach Risk Assessment Form (see Appendix C) to the DPO.

The key officers involved should be proportionate to the type of breach. For instance, a minor breach may require the following:

- Assistant Director
- Line Manager
- DPO
- SIRO

A serious breach, whether in terms of size of breach, or sensitivity of information, should comprise the following:

- Managing Director
- Strategic Director
- Assistant Director/s

Responsibility rests with the Assistant Director, or their nominated deputy, in considering the action to be taken to:

- Protect the interests of the customer
- Ensure the continuing delivery of the service
- Protect the interests of the councils

Breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or

closing a compromised section of the network, finding a lost piece of equipment, or simply changing access codes. Establish whether losses can be recovered and damage can be limited.

Fully assess the risk in terms of the potential adverse consequences for individuals. How serious or substantial are the consequences and how likely are they to happen?

Notifying the Information Commissioner's Office (ICO)

The GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office.

In the case of a personal data breach the Council "*shall without undue delay and, where feasible, not later than 72 hours after having become aware of it*", notify the ICO, *"unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".* Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

The GDPR states that a personal data breach should be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this is done on a case by case basis. If there is not a risk to rights and freedoms, the ICO does not need to be notified.

After carrying out a full assessment of the risk, the decision as to whether or not to inform the ICO would normally rest with the Data Protection Officer in consultation with the Leadership Team. However, there may be circumstances where the decision to report the breach is the responsibility of the Managing Director e.g. where the information lost is owned by a number of services, or where the implications of the breach would seriously affect the reputation of the councils as a whole.

The Assistant Director will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

The notification to the ICO shall at least:

a) Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
b) Communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained
c) Describe the likely consequences of the personal data breach
d) Describe the measures taken or proposed to be taken by the councils to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The Council shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the GDPR.

The new legislation has increased monetary penalties. Failing to notify a breach when required to do so can result in a proportionately significant fine of up to £17mill.

Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Council shall communicate the breach to the data subject without delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are:

- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation

When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, the above example of damages are likely to occur.

The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) above.

The communication to the data subject shall not be required if any of the following conditions are met:

I. The councils have implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
II. The councils have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise
III. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Consideration also needs to be given to any prospective equality issues that may arise from a breach e.g. the vulnerability of an individual affected by the breach.

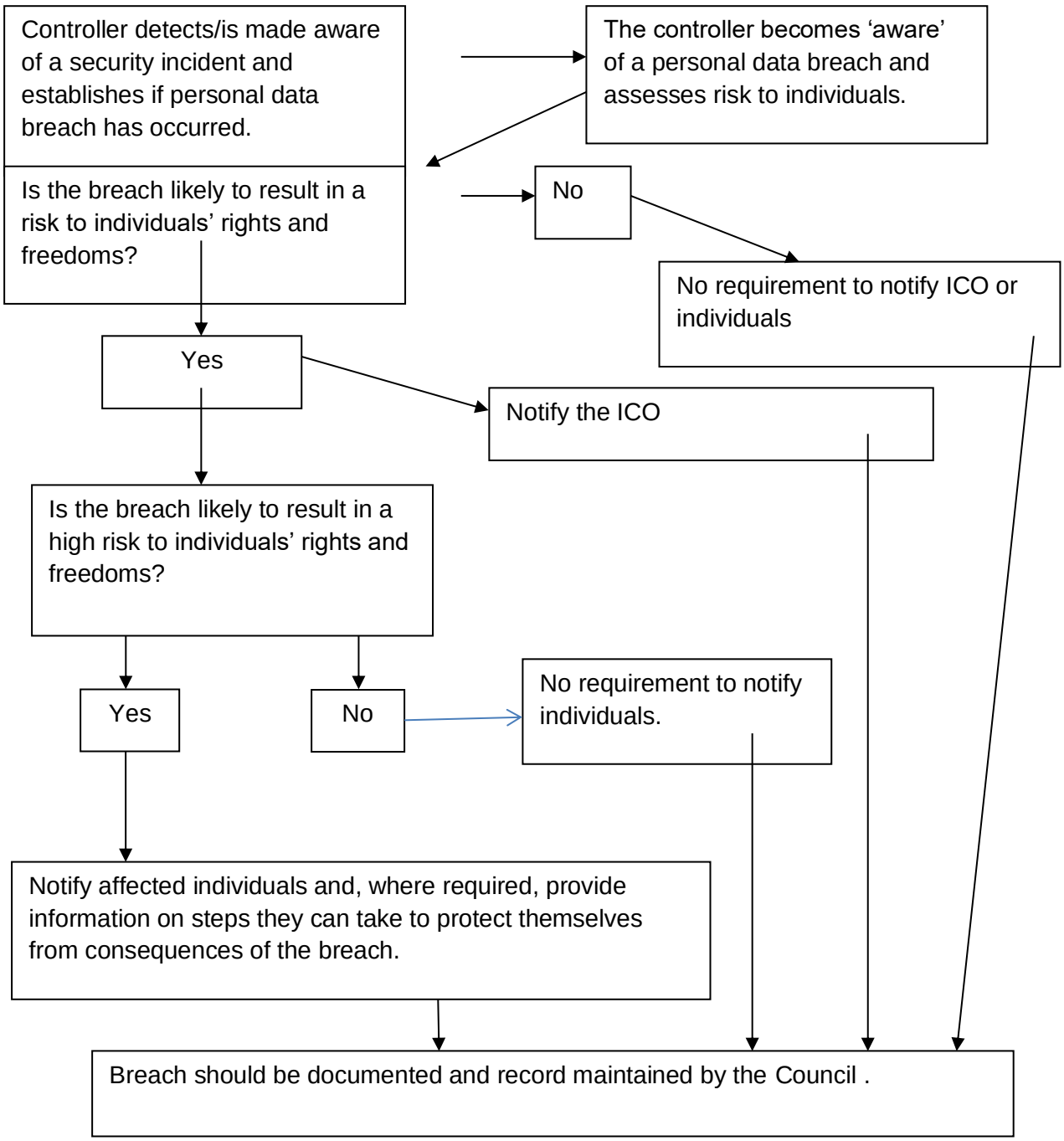
Post breach evaluation

Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on 'business as usual' may not be acceptable if systems, policies or allocation of responsibilities was found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and recorded so the council can be seen to have reacted in a responsible manner.

Those investigations into the cause of the loss of data should consider any staff capability or training issues that may be indicated and where appropriate, action may be considered under the council's disciplinary procedure.

If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future.

Flow chart showing notification requirements



APPENDIX C

DATA SECURITY BREACH RISK ASSESSMENT FORM	
Information Asset Owner/Deputy Officer	
Dept./Section	
What type of data is involved?	
How sensitive is it?	*Some data is sensitive because of its very personal nature e.g. health records whilst other data types are sensitive because of what might happen if it is misused (bank account details)*
If data has been lost or stolen are there any protections in place such as encryption?	
What has happened to the data?	*If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk*
Regardless of what has happened to the data, what could the data tell a third party about the individual?	*Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.*
How many individuals' personal data are affected by the breach?	*It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.*
Who are the individuals whose data has been breached?	*Whether they are staff, customers or suppliers will to some extent determine the level of risk posed by the breach and, therefore your actions in attempting to mitigate those risks*
What harm can come to those individuals?	*Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?*
Are there wide consequences to consider such as a risk to public health or loss of public	

DATA SECURITY BREACH RISK ASSESSMENT FORM	
confidence to an important service you provide?	
If an individual's bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use	
Signed:	
Dated:	

Once completed this form should be passed to the Data protection Officer.