Annex C

DATA SECURITY BREACH MANAGEMENT POLICY AND PROCEDURE

1. INTRODUCTION

1.1 Surrey Heath Borough Council (SHBC) processes personal data and must respond appropriately against unauthorised or unlawful processing, against loss, destruction of or damage to data.

1.2 Under the Data Protection Act 1998, Surrey Heath Borough Council is a Data Controller. This is a "person" who determines the purposes for which and the manner in which any personal data are, or are not to be processed. The seventh Data Protection principle states that organisations, which process personal data, must take "appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". This means SHBC has a responsibility to ensure appropriate security of all personal data it holds.

The Data Protection Act 1998 says **personal data** concerns the identification of living individuals. Information, described as Sensitive Personal Information, must have extra care taken. The definition of Sensitive Personal Information is:

- 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 by him/her of an offence or any proceedings for any offence committed or alleged to have been committed
- the disposal of such proceeding or the sentence of any court in the proceedings.

1.3 As well as defining SHBC's policy, this procedure lays out the actions, which should be taken once a breach has occurred.

2. SCOPE

2.1 This policy and procedure applies to all users of SHBC's information, data, information systems and the Council's physical buildings. It applies to not only staff and members but also contractors, agency staff, service providers, consultants and anyone else engaged to work in the organisation and encompasses data, information, software, systems, and paper documents.

2.2 This policy should be read in conjunction with other relevant policies, including but not limited to:

- Information Governance Strategy and Policy
- Data Protection Policy

- Information Security Policy
- Email Management Policy
- Disciplinary Policy
- Social Media Policy
- Whistle-blowing Policy and Procedure

All staff, including all new starters, must read and sign that they have read this policy as this forms part of the Staff Terms and Conditions.

3. TYPES OF BREACH

3.1 A number of factors could cause data protection breaches. The following is a list of examples but it is not exhaustive and there may be others which will need to be considered at the time of the breach:

- loss or theft of data
- loss or theft of equipment on which data is stored
- inappropriate access controls allowing unauthorised use, both electronic and paper
- equipment failure
- human error in dealing with personal information including both electronic and paper
- unforeseen circumstances such as fire or flood
- hacking attack on the Council's ICT systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- unauthorised access into secure areas

4. NOTIFICATION OF BREACHES

4.1 The person who discovers/receives a report of a breach must inform the Information Governance Manager forthwith. If the breach is discovered due to whistle blowing and the reporter does not wish to tell the Information Governance Manager then an/the appropriate manager must tell the Information Governance Manager. In the absence of the Information Governance Manager then the Monitoring Officer (Head of Legal) should be informed. If the breach occurs, or is discovered outside normal working hours, notification must happen as soon as is practicable.

4.2 The Information Governance Manager or in their absence the Monitoring Officer, will then decide whether to involve other departments e.g. Human Resources, ICT.

4.3 The Information Governance Manager will maintain a log with the details of all breaches. This will include who the Lead Investigator is, when the breach occurred, who is involved and what action must be taken after the breach.

4.4 The Information Governance Manager will, in consultation with others, if necessary, decide who the Lead Investigator should be, who needs to be involved and will work with them to manage the breach. The Information Governance Manager is responsible for advising services on assessing the impact of any data breach of the Data Protection Act. This can include recommendations to restore data security.

4.5 The Lead Investigator could be any of the following:

- a member of Audit and Investigations
- Executive Head
- Monitoring Officer
- Information Governance Manager
- a member of Human Resources
- a combination of the above

4.6 The Information Governance Manager or Monitoring Officer will decide whom to notify.

4.7 If the breach involves any IT systems, the ICT Manager (or in the manager's absence ICT Systems Team) must be informed immediately.

4.8 The Senior Information Risk Owner (SIRO) (the Executive Head of Finance) will be told of any breaches at the Information Governance Managers regular review meetings. For serious breaches (i.e. the extent of the 'damage'), the SIRO must be informed immediately, the Chief Executive will be made aware. A decision will be taken as to whether to inform the Information Commissioner's Office. The final decision on notifying the Information Commissioner's Office rests with the SIRO. The process will consider the number of people affected and/or the seriousness of the consequences.

4.9 The Lead Investigator/SIRO must also consider whether the police need to be informed. This could be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. If credit card numbers are lost then tell the appropriate bankcard provider.

4.10 Consider notifying all staff if thought necessary or will stop additional breaches.

4.11 Notification should have a clear purpose. This can be to gather information, advice or allow the appropriate regulatory bodies to perform their functions, and deal with complaints. It can also enable individuals affected to take steps to protect themselves.

4.12 Answering the following questions will assist you in deciding whether to notify people and who:

- can notification help you meet your security obligations with regard to the seventh Data Protection principle? See 1.2
- can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- consider how notification can be made appropriate for particular groups of individuals, for example, if children or vulnerable adults are involved. Also, consider the appropriate method of communication. Always bear in mind the security of the medium as well as the urgency of the situation.
- consider the danger of 'over notifying'. Not every incident will warrant notification and notifying the whole customer base of an issue affecting only a few customers may well cause disproportionate enquiries, upset and work. It may also cause unwarranted release of data (secondary breach).

- as well as notifying the Information Commissioner's Office, other regulatory bodies may need to be informed.
-

5. CONTAINMENT

5.1 At the same time as notification is happening, containment and recovery must also happen.

5.2 The Lead Investigator must ascertain whether the breach is still occurring. If so, it must be stopped immediately and minimise the effect of the breach. This will involve liaison with appropriate staff. Examples might be the ICT Manager authorising the shut down of a computer system or stopping the delivery of mail.

5.3 Media and Marketing may need telling of a breach if there is a possibility of information published on the Internet or the press told and their assistance is required in managing a media response.

6. ASSESSING THE RISKS

6.1 Some data security breaches will not lead to risks beyond the possible inconvenience to those who use the data to do their job, for example if a laptop is irreparably damaged or lost, in line with the Information Security Policy, it is encrypted, and no data is stored on the device. There will be a monetary cost to the Council by the loss of the device but not a security breach.

6.2 Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of customer data, whereby the data may be used to commit identity fraud.

6.3 Before deciding on what steps are necessary, and after immediate containment, an assessment of the risks, which may be associated with the breach, must take place. One of the key assessments is the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. A key part of the definition of a breach is harm and distress i.e. what harm and distress will the breach cause; in particular to the individuals concerned but could include the Council.

6.4 Although there is no definition of a 'serious breach' a decision will have to be made as to whether a breach is 'serious'. The following should be considered in making the decision before reporting:

- has harm or distress been caused to data subjects – for example identity theft through loss of details on a passport
- volume of data lost – for example unencrypted laptop with lots of individuals personal details
- loss of sensitive data for example a manual file with medical, criminal and details of a vulnerable child or an individual

6.5 As part of the risk, consider whether the person/people whose information has been breached should be informed. The guidance from the Information Commissioner is that they should be informed unless to inform them will cause additional distress/stress.

6.6 If after conducting a risk assessment on whether to notify the people whose data has been compromised and it is considered appropriate to contact them, consider the following:

- what is the most appropriate method of communication? Always bear in mind the security of the medium as well as the urgency of the situation
- the notification should include as a minimum, a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach
- give the individuals clear advice on what they should do to protect themselves and what the Council are willing to do on their behalf
- provide a means of contacting SHBC for further information. This could include a named individual, a helpline number, a web page or a combination of all of these.

6.7 Helpful tips for assessment of risks:

- what type of data is involved?
- how sensitive is it? Is it sensitive personal details as defined by the Data Protection Act 1998 (e.g. housing benefits) or other data types which are sensitive because of what might happen if it is misused (e.g. bank account details). See 1.2 for a definition of sensitive personal information
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data?
- can the data be restored or recreated?
- how usable is the lost data?
- if data has been stolen, could it 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
- 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 is 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? Are they staff, customers, clients or suppliers?
- what harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these and other aspects of their life?
- are there wider consequences to consider such as a risk to loss of public confidence in one of the service areas?
- if an individual's bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use

7. INVESTIGATION, EVALUATION AND RESPONSE

7.1 In most cases, the next stage would be for the Lead Investigator to fully investigate the breach. The Lead Investigator should ascertain whose data was involved in the breach, the person or people responsible for the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

7.2 Breaches will require not just an initial investigation, decision on the severity and containment of the situation but also a recovery plan including, where necessary damage limitation. This will often involve input from ICT, HR, Legal, Information Governance and the appropriate department. In some cases contact with external stakeholders or suppliers may be required.

7.3 The Information Governance Manager will assist the Lead Investigator, where necessary. This could include informing the Information Commissioner's Office, calculating the severity of the incident, collating reports, implementing actions from the Information Governance report.

7.4 The Lead Investigator will establish the questions for interviews and then meet with the participants. This could be (but is not limited to or necessarily all of them) witnesses, victims and perpetrators, senior managers.

7.5 The Lead Investigator will identify if there is a need for expert advice from either professional advisers or Legal Services.

7.6 Issues to be addressed during the investigation will include:

- the date when the breach occurred
- the date when the breach was identified to SHBC and to whom
- the type of data and the number of records involved
- its sensitivity
- the circumstances of the release
- what protection is in place (for example encryption)
- what has happened to the data
- whether the data could be put to any illegal or inappropriate use
- how many people are affected
- what group of people has been affected (the public, suppliers etc)
- whether there are wider consequences of the breach

7.7 The lead investigator will keep an electronic record of all activities during the investigation. This could include the actions taken to mitigate the breach and lessons learnt. The reason for this is if there are actions by the police, Information Commissioner's Office, legal proceedings or Audit, the records will be required to be shared.

7.8 There could be a number of investigations going on at any one time for example by Human Resources and ICT.

7.9 Begin investigation immediately on receipt of notification. Complete urgently and wherever possible within 24 hours of the breach being discovered/reported. Carry out, if necessary a further review of the causes of the breach and recommendations for future improvements once the matter has been resolved

7.10 If systemic or on-going problems are identified, draw up an action plan to correct. If the breach warrants a disciplinary investigation (for example due to

negligence), the Lead Investigator should pass on any relevant information to Human Resources

7.11 The Lead Investigator should produce a report for the SIRO.

7.12 The report must address the following:

- establish the facts (including those that may be disputed)
- include a chronology of events including the containment, recovery and how the breach has been investigated
- a risk analysis
- a commentary of the weight of evidence
- action to minimise/mitigate effect on individuals involved including whether the victims have been informed
- whether any other regulatory body and been informed and their response
- recommendations to reduce the chance of the same breach happening again

8. REVIEW

8.1 A policy review will take place annually or after a serious breach, legislative changes, important changes in case law, or guidance.