Further to your Information request FOI65067 please find your questions and our responses below:

I am interested in information security.
I would therefore like to request:

• your information/data security policy;

**Response: This is a Section 17 Refusal Notice. S21 (Information is available by other means) exemption has been applied.**

This Information is available on the RBWM web site please go to:  
http://www.rbwm.gov.uk/web/info-security.htm

• details of any training/information given to staff on security and data-handling.

**Response: There are three security training courses. Staff are given course profiles before they attend, please see attached.**

This concludes your request FOI65067.

If you require translation of the information you have been sent please do not hesitate to contact us.

If you are unhappy with the information we have provided in response to your request please write to:

Information Management Team Manager  
Royal Borough of Windsor & Maidenhead  
Town Hall, St Ives Road  
Maidenhead  
SL6 1RF

or send an e-mail to martin.tubbs@rbwm.gov.uk

We are proud to be one of the leading authorities in England for consistently responding to information requests within the 20 working days set down by statute. Information about our performance and summaries of requests received can be found on our website:

http://www.rbwm.gov.uk/web/foi_information_requests.htm

We are keen to hear about your experience with the Information Management Team here at the Royal Borough of Windsor & Maidenhead and look forward to receiving any comments you have about the way your information request was processed.

Please send any feedback to the Information Management Team Manager either by e-mail martin.tubbs@rbwm.gov.uk or in writing to the address above.
Course Title: Information Security Protection

Overview:
This two and a half hour course provides you with a basic understanding of security risk and how to protect Council information and computer equipment. It covers the dangers of security breaches and how to report them, physical security, IT access, cyber attacks, remote working, how to handle and protect information.

Extra security measures you must take when accessing the Government IT network and when using GCSx encrypted email are explained. These Government services allow you to exchange information more safely with other Councils and also with some Government Departments and agencies.

Course completion is a first step towards gaining Government Baseline Security authorisation, needed before you can access the Government IT network.

Real-life security examples are built into the course. Also a multiple choice test about the extra security rules used when accessing the Government IT.

Duration: 2 ½ hours

Who is the course for?
Everyone who does work for the Council including Councillors, Directors, Heads of Service, Managers, Team Leaders, Contractors, Consultants and Agency Workers.

Course Pre-requisites: None

Objectives:
To provide a basic understanding of:
1. The dangers of security breaches and how to report them
2. The main ways to reduce the risk of security breaches in these areas:
   a. physical security
   b. IT access security and cyber attacks
   c. remote working
   d. handling and protecting information, and
   e. accessing the Government IT network online or by using GCSx email.

Learning Outcomes: An understanding of
(a) some of the security risks you are exposed to, and how to identify them
(b) the most important security precautions you must take when accessing Council information, and
(c) the extra security measures you must take when using the Government IT network.

Supports competencies:

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>EMPLOYEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant Improvement - setting high standards</td>
<td>Customer Led - delivering to agreed standards</td>
</tr>
<tr>
<td>Leadership - taking responsibility</td>
<td>Working Together - Understanding and supporting others</td>
</tr>
</tbody>
</table>

Other related workshops:
The Data Protection Act Overview Course
Course Title: Data Protection Act

Overview:
This 90 minute course covers the main aspects of the Data Protection Act 1998.

The session commences with an appraisal of a number of actual Data Protection breaches, their consequences and how they could have been avoided.

Basic terminology is explained, and the Eight Principles, and Schedules 2 & 3 are covered.

Data Subjects’ Rights and RBWM employees’ obligations are discussed.

Exercises include:
- Obtaining information and Privacy Notices
- What to do if a police officer calls
- What to do if someone requests a colleagues contact details
- When it is OK to share information

Reference is made to the complementary Information Security training.

Duration: 90 minutes

Who is the course for?
Everyone who does work for the Council including Councillors, Directors, Heads of Service, Managers, Team Leaders, Contractors, Consultants and Agency Workers.

Course Pre-requisites: None

Objectives:
To provide a basic understanding of:
1. The importance of compliance with the Data Protection Act 1998
2. How compliance can be improved
3. The consequences of compliance failures:
   a. training
   b. enforcement notices
   c. fines
   d. criminal prosecution

Learning Outcomes: An understanding of
(a) Data Protection compliance in the workplace
(b) Data subjects’ rights and how they can be exercised.

Supports competencies:

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>EMPLOYEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant Improvement - setting high standards</td>
<td>Customer Led - delivering to agreed standards</td>
</tr>
<tr>
<td>Leadership - taking responsibility</td>
<td>Working Together - Understanding and supporting others</td>
</tr>
</tbody>
</table>

Other related courses:

Information Protection Course
Course Title:  Data Protection Act and Information Security Protection for Managers

Overview:
This two and a half hour course provides a comprehensive overview of the Data protection Act 1998, and the Council’s security standards, policies and procedures.

The first hour explains past Data Protection breaches, their consequences, and how they might have been avoided. Basic terminology is explained, and what you need to do to comply with the Eight Principles of the Act. Data Subjects’ rights and Council employees’ obligations are also discussed.

The second half of the course provides you with a basic understanding of security risk and how to protect Council information and computer equipment. It covers the dangers of security breaches and how to report them; physical security; IT access; cyber-attacks; remote working; and how to handle and protect information. Real-life examples are built into the course.

Duration:  Two and a half hours

Who is the course for?
Directors, Heads of Service, Managers and Team Leaders

Course Pre-requisites:  None

Objectives:
To provide a basic understanding of:
1. the importance of compliance with the Data Protection Act 1998
2. how compliance can be improved
3. to provide a basic understanding of:
   a. the dangers of security breaches and how to report them
   b. how to reduce the risk of security breaches.

Learning Outcomes:  An understanding of:
(a) Data Protection Act 1998 compliance in and out of the workplace
(b) the security risks you are exposed to, and how to identify them
(c) the security policies and procedures you must comply with.

Supports competencies:

<table>
<thead>
<tr>
<th>MANAGEMENT</th>
<th>EMPLOYEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant Improvement - setting high standards</td>
<td>Customer Led - delivering to agreed standards</td>
</tr>
<tr>
<td>Leadership - taking responsibility</td>
<td>Working Together - Understanding and supporting others</td>
</tr>
</tbody>
</table>

Other related courses:
Full Data Protection Act Course
Full Information Security Protection Course