IT ESSENTIALS – Introduction To IT Facilities for New Staff Members (ST010)
Main IT System-Applications Used At Royal Holloway

The table below lists the main IT applications you are likely to come across at the College.

Most of these can be accessed from the iQuad College systems web page at: www.rhul.ac.uk/iquad/collegesystems/

<table>
<thead>
<tr>
<th>System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner</td>
<td>The College’s Student Record System</td>
</tr>
<tr>
<td>Campus Connect</td>
<td>A student facility that pulls together key information from a number of</td>
</tr>
<tr>
<td>also known as</td>
<td>sources, including fees, exams, and courses (staff also have a version)</td>
</tr>
<tr>
<td>Portal</td>
<td>campus-connect.rhul.ac.uk OR portal.rhul.ac.uk</td>
</tr>
<tr>
<td>Contensis</td>
<td>The Content Management System used to produce College web pages wcms.rhul.ac.uk</td>
</tr>
<tr>
<td>EMS (FootPrints)</td>
<td>The application running the college enquiry management system, including IT</td>
</tr>
<tr>
<td></td>
<td>Service Desk. More info and Login link: <a href="http://www.rhul.ac.uk/it">www.rhul.ac.uk/it</a></td>
</tr>
<tr>
<td>Moodle</td>
<td>The Virtual Learning Environment (VLE) used in the College moodle.rhul.ac.uk</td>
</tr>
<tr>
<td>MyView</td>
<td>The system used to view pay and make (hourly pay)claims</td>
</tr>
<tr>
<td>Raisers Edge</td>
<td>The College’s Alumni record system</td>
</tr>
<tr>
<td>Web Timetables</td>
<td>Used to view lecture theatre and seminar rooms bookings</td>
</tr>
<tr>
<td></td>
<td>rhul.ac.uk/timetable</td>
</tr>
<tr>
<td>Agresso</td>
<td>The College’s finance system</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Webmail</td>
<td>Gives access to College e-mails via the Internet mail.rhul.ac.uk</td>
</tr>
</tbody>
</table>
New Staff IT Induction

1. Help and Support

A range of IT help is available should you need it. This can be obtained from the following:

Put a call into the IT Service Desk using one of the following methods:

- Email: itservicedesk@rhul.ac.uk
- Web: enquirymanagement.royalholloway.ac.uk
- Telephone: 01784 41 4321

Visit the IT Service Desk in Davison Library Monday to Friday from 09:00 until 17:00

For Laptop and Mobile Device Support visit Davison Library IT support office next to the main Library enquiry desk. To view the most up-to-date timetable please visit:
https://intranet.royalholloway.ac.uk/students/help-support/it-services/getting-help-with-it.aspx

2. The IT Department’s Homepage

The IT Department’s homepage (http://www.rhul.ac.uk/IT/) offers a range of useful information and help.

Here you can find information relating to Contact Details/Getting help, Service status, Webmail, Training, Web safety & Antivirus, FAQs.
3. Logging on to a PC in your Area

To log on to the facilities provided by the IT Department throughout Campus you need to know:

a. Your computer username.
   This consists of 4 letters and 3 digits, e.g. ucaa124 and is unique to each member of College.

b. Your password.
   Note: Your username identifies you as a bona fide member of the College and in conjunction with your password allows you to access the College Network.

4. Why log on to the College Network

Logging onto the College Network gives you access to a number of essential facilities including:

- Any departmental shared folders that are accessible by you, e.g. the (N:) drive. As these are backed up you are strongly recommended to use them wherever possible.

- Your own personal network space, called the (Y:) drive, which is backed up and so strongly recommended to be used.

- Your College e-mail account.

- Any networked printers that your PC can access.


- Library facilities, e.g. access to the Library catalogue.

- Webmail for accessing your College e-mail from off Campus.

- Access to restricted material when working off-Campus via Campus Anywhere (VPN).

5. Your Computer Password

To maintain security your password should adhere to the College’s Password Policy (see page 39). To summarise its content, this includes that your password must be: A minimum of 8 characters.

- Not a word written down anywhere, or be a Royal Holloway related word.

- A mixture of upper and lowercase alphabetical characters, numbers, and basic punctuation.
Not something that can be guessed easily by others, e.g. your date of birth or car registration number, and not written down anywhere.

It is good practice to log off your computer/laptop when you are not using it as this can prevent others accessing your files and working under your identity. Similarly, if you are leaving your computer/laptop for a long period of time, e.g. overnight, it is recommended that you close it down in order to save electricity and also protect your data from being accessed.

Do remember that College Regulations prohibit you from divulging your password to anyone else. Therefore, if there seems to be a need in your department for sharing systems (for example to share folders located on someone’s PC) the IT Service Desk should be able to offer an alternative, and so avoid compromising security.

To access the College policies relating to your use of IT within the College please visit: https://intranet.royalholloway.ac.uk/it/tos/regulations.aspx

Then select the Information Technology and Library tab.

6. Changing your Password from your Office PC

You can change easily your password from your office PC. To do this:

a. Ensure that you are logged on to your PC.
b. Press [Ctrl]+[Alt]+[Delete] on the keyboard.

c. A window displays with a range of options.
d. Click on Change a Password to display a second window containing username and password panels.
e. Ensure that the username in the top panel display the username for which you wish to change the password.
f. Click within the Old password panel and enter your current password, remembering that passwords are case sensitive. For security reasons you will just see a series of dots.
g. Click within the New password panel and type in the new password you wish to use; again you will just see a series of dots as you type. Remember that passwords are case sensitive.
h. Click in the Confirm password panel and enter the same password again; you will just see a series of dots as you type.

If you have done everything correctly you will receive a message telling you that Your password has been changed; click on OK to close the window.

Or
If you have done anything wrong, such as typing different passwords in the New password and Confirm password panels, you will receive an error message.

i. Take note of its content, then click on OK. You will be returned to the window containing the username and password panels where you can re-enter your passwords. When you have finished click on to change the password and to close the window.

7. Changing your password using the Password Manager

Unlike the [Ctrl]+[Alt]+[Delete] method covered in the previous section, the Password Manager offers the facility for you to change your password (even if you have forgotten it!) from anywhere with an Internet Connection.

However, do note that being able to reset a forgotten password is dependent on you having already set up three security questions (see step (i)). It is therefore useful to do this before you need to use this facility!

To use the Password Manager:

a. Open a browser, e.g. Internet Explorer

b. Open the following web page: http://passwordmanager.rhul.ac.uk/

c. In the Enter your first, last, partial, or logon name: panel enter your username (e.g. zvaa666).

d. Click on Search to display a list of options.

Or

e. If you cannot remember your username:
   (1) Enter your name using the format first name followed by family name.
   (2) Click on Search.
   (3) If a list of possible College members displays click on the username link for your entry.

f. A list of options displays.
i. If the Register with Password Manager option displays (1)
   Click on the Register with Password Manager link.
(2) Enter your password into the Password: panel.
(3) Click on Next.
(4) Select and answer any 3 security questions from the available list. These will be used in the future to identify you to the Password Manager facility, and so you must ensure your answers are memorable.
(5) When finished click on Finish.
(6) Click on the Home page link to return to the Password Manager’s home page.

If the Manage My Passwords option displays
a. Click on the Manage My Passwords link.
b. Enter your password into the Password: panel.
c. In the Enter new password: panel enter the new password you wish to change to, remembering that passwords are case-sensitive.
d. In the Confirm new password: panel enter the new password again.
e. When you have finished click on Finish.

Dealing with a Forgotten Password
Once you have registered with the Password Manager you can then use it to reset a forgotten password from both on and off Campus. To do this:

a. Open the web page http://passwordmanager.rhul.ac.uk to display the Password Manager.
b. Click on the Forgot My Password link.
   Note: This option will not display if you have not completed the security questions as part of registering with the Password Manager facility.
c. Answer the security questions.
d. Click on Next.
e. In the Enter new password: panel enter the password you now wish to use, remembering that passwords are case-sensitive.
f. In the Confirm new password: panel enter the password again.
g. When you have finished click on Finish.
8. Locations for saving your work

To enable effective, backed-up, storage of your work you are likely to have access to one or more of the following drives:

(Y:) drive:
This is a backed-up drive, accessible by only you that can be used for personal work-related data. Everyone on Campus, including students, have a (Y:) drive.

When using your own or external equipment this can be accessed by mapping to:
PC: \mydata.rhul.ac.uk\Home
Mac: smb://mydata.rhul.ac.uk/home

Departmental Shared drive – frequently referred to as the (N:) drive
This is a backed up drive that is accessible by a number of users within a department or area to enable the sharing of work.

When using your own or external equipment this can be accessed by mapping to:
PC: \ourdata.rhul.ac.uk\departments
Mac: smb://ourdata.rhul.ac.uk/departments

Cross-Departmental Shared drive – frequently referred to as the (M:) drive
This is a backed up drive that is used to enable shared working across departments e.g. cross-departmental work.

When using your own or external equipment this can be accessed by mapping to:
PC: \ourdata.rhul.ac.uk\workinggroups
Mac: smb://ourdata.rhul.ac.uk/workinggroups

Mapping a Drive
Details of how you can map to the above drives, e.g. on your home computer can be found at:
http://www.rhul.ac.uk/it/faq/itfaqs/networkconnectivity/mapdrive.aspx

9. Accessing Facilities Off-Campus with Campus Anywhere (VPN)

Some College facilities are restricted to on-Campus access only, e.g. some departmental course notes, online journals/databases, your departmental shared drives, and your (Y:) drive.

If you wish to access these facilities from off-Campus using the Internet you will need to create a connection to the College using the College's Campus Anywhere VPN (Virtual Private Network) system. For details of how to setup this service please visit:
http://www.rhul.ac.uk/IT/CampusAnywhere

10. Accessing your office PC away from Campus

By using Remote Desktop Connection (RDC), you can access your office PC from anywhere using the Internet, and then work on it as if you were actually in your office. This can be very useful if you are unable to get to College, for example during times of adverse weather.
To use this you will need:

- To contact the IT Service Desk and request them to enable Remote Desktop Connection on your office PC
- Your Office PC’s PC Name (e.g. CCPC123) and IP address (e.g. 134.219.123.123). This is normally located on a sticky label on your PC.

Note: When using RDC with the PC Name you will need to first turn on Campus Anywhere/VPN (see section 9 above); if using the IP address you will not need to do this.

For details of accessing and using RDC please contact the IT Service Desk.

11. Securing your Work

It is clearly important that you protect the work you produce. To help you with this do take note of the following points:

- To help prevent loss of work, for example if the mains power drops-out you are strongly advised to save your work VERY regularly.

NEVER save any College related work, especially confidential and important work to the PC’s (C:) drive or a USB memory drive. This is because:

- The work will be lost if the drive fails – instead save it to your (Y:) drive or departmental shared drive (N:) drive (see section 8), as these are regularly backed up

- If the PC is stolen, or a USB memory drive lost, it could have consequences under the Data Protection Act

When working on larger documents you are recommended to change the filename as you progress, e.g. Handbook v1.doc, Handbook v2.doc etc.
By doing this, for example after every hour of concerted work, you will have a series of incremental files that if one corrupts you can go back to a previous version and so will not have lost the entire work.

Where available do follow your departmental backup procedures.

If working on a document opened via an e-mail attachment ensure you save it to a know location, e.g. a departmental shared drive, before progressing – if you don’t the file will be saved to a temporary folder on the (C:) drive, which is deleted when Outlook closes!

Also, if you are considering saving any College related work to one of the cloud based/externally hosted storage areas we strongly advise you seek guidance from the College Secretary, so as to avoid any potential data loss or breaches of the Data Protection Act. For further details see the Cloud Services: RHUL Code of Practice document on page 29 of these Session Notes.

12. Laptop Users

In addition to the points previously made about securing your work (see section 11), when using a laptop you should also consider the following:
Do consider the impact of losing the laptop, both in respect to the loss of your work and the Data Protection Act.
Ensure that you always secure it using, for example, a Kensington lock.
Always lock the door when your office is unoccupied.
Never keep backups with the laptop (to prevent both being lost/stolen!).

13. Using your Departmental Shared Drive

Your Departmental Shared Drive (frequently referred to as the (N:) drive) can help enhance your collaborative working with other members of your department/area.

By making effective use of this backed-up storage area you can:
- Produce documents with other members of your department/area
- Enable documents to be easily accessed by other members, and teams, within your department/area

When using this drive you are recommended to save your work within suitably named folders.

14. Virus Control

Computer viruses are programs designed to replicate and spread, often without indicating that they exist. Some viruses do little damage, but in extreme cases viruses can damage files and computer disks, resulting in the loss of any work that was stored on them.

All College PCs should be protected by Sophos antivirus software. Because new viruses are being created all the time this should be set to automatically download updates as they become available.

There are a range of precautions you must take to make sure that computer viruses do not damage your work:
- a. ENSURE your own computer/laptop has an up-to-date anti-virus application installed.
- b. ENSURE update patches e.g. Windows and Office updates are kept fully up-to-date on your own computer/laptop.
- c. Ensure that your antivirus program IS setup to provide background protection, so that it automatically scans every file you open or download via the Web.
- d. NEVER open a file attachment from a recipient whose name you do not recognise.
- e. Don’t open a file attachment from within an e-mail which looks suspicious even if you may know the name of the sender - get advice from the IT Service Desk first.
- f. Keep up-to-date copies of your files in more than one location so that you have another copy if one should become infected.

It should be noted that the Sophos antivirus software is available to download FREE to all College members for use on their own computer/laptop.
Further details can be accessed from the Web safety & antivirus link in the centre panel of the IT Department’s IT for Staff homepage (see Section 2) or visit: http://www.rhul.ac.uk/it/onlinesafety.aspx

15. Software Licenses

It is important that you adhere to the software license regulations. Therefore you should consider the following when considering installing your own software on any College PC:
   a. The College provides Microsoft Office as standard on all office PCs.
   b. You can only install your own software on a College computer/laptop if you have a valid license for it.
   c. Contact the IT Service Desk for details on purchasing software and license agreements.
   d. If you need software installed in an Open-Access PC Lab you will need to contact the IT Service Desk well in advanced of when it is needed.
      Note: It is frequently difficult to add software to the PC Lab build during the academic year.

16. The STAFF INTRANET

It is important to note that members of College must not send e-mails to large numbers of College members, e.g. all staff, as this can create a significant number of complaints.

Instead, when wishing to contact members of staff (students can also access it) you should use the STAFF INTRANET.

To view the STAFF INTRANET, click on the Staff button at the top of the College homepage (www.rhul.ac.uk).

To send a message for display on the STAFF INTRANET:
   a. Point to the News and events link at the left of the black bar at the top of the window.
   b. Click on See or post on the campus noticeboard at the bottom of the menu that displays.
   c. Then complete the Submit a post panel on the right of the page that displays.
   d. When you have finished click on Post towards the panel’s bottom right
17. The STUDENT INTRANET

The STUDENT INTRANET enables both students and members of staff to communicate with students.

Students can view the STUDENT INTRANET: Once they log on to any of the Open-Access PCs.

Under the Campus Noticeboard (left-hand) heading on Campus Connect, the College Portal (campus-connect.rhul.ac.uk or portal.rhul.ac.uk). By clicking on the Students button towards the top centre of the College homepage.

To submit a message for display on the STUDENT INTRANET:
   a. Point to the News and events link at the left of the black bar at the top of the window.
   b. Click on Read or post on the campus noticeboard towards the bottom of the menu that displays.
   c. Then complete the Submit a post panel on the right of the page that displays.
   d. When you have finished click on Post towards the panel’s bottom right.

18. E-mail at Royal Holloway

Your College e-mail account can be accessed in a variety of ways, including:
   From your office PC using Microsoft Outlook 2010 (part of Office 2010).
   From a laptop or home computer using Outlook 2010 if Office 2010 is installed. From a laptop/computer connected to the Internet anywhere in the world using Webmail.
   From a Smartphone, iPad etc.

College e-mail Address Formats
It is useful to understand how e-mail addresses at Royal Holloway are constructed. The College e-mail address rhul.ac.uk stands for:
   rhul: Royal Holloway University of London
   ac: Academic Community
   uk: United Kingdom

There are three main structures used at Royal Holloway for e-mail addresses. These are:

<table>
<thead>
<tr>
<th>E-mail Address Format</th>
<th>Used by</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:forename.surname@rhul.ac.uk">forename.surname@rhul.ac.uk</a> e.g. <a href="mailto:ann.nonymouse@rhul.ac.uk">ann.nonymouse@rhul.ac.uk</a></td>
<td>Generally for all new staff</td>
</tr>
</tbody>
</table>
The table below outlines the email formats for staff and students:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:initial.surname@rhul.ac.uk">initial.surname@rhul.ac.uk</a> e.g. <a href="mailto:a.nonymouse@rhul.ac.uk">a.nonymouse@rhul.ac.uk</a></td>
<td>Staff employed prior to 1999</td>
</tr>
<tr>
<td><a href="mailto:forename.surname.entry-year@live.rhul.ac.uk">forename.surname.entry-year@live.rhul.ac.uk</a> e.g. <a href="mailto:ann.nonymouse.2009@live.rhul.ac.uk">ann.nonymouse.2009@live.rhul.ac.uk</a></td>
<td>All students</td>
</tr>
</tbody>
</table>

Note: Although these are the main formats used others may be employed where 'that' one is already in use, e.g. forename.initial.surname@rhul.ac.uk

Staff and students’ mailboxes are hosted by Microsoft, and have 50GB of space.

You should note that the Computer Science and Earth Sciences departments use their own email servers and hence their email address may differ from the @rhul.ac.uk address. Also, they may not use Microsoft Outlook for sending/receiving e-mails, and therefore may not be able to use some of the features included with Outlook.

19. Royal Holloway E-mail Guidelines

The College’s E-mail Guidelines, which are included on page 21 of these Session Notes, have been drawn up as a result of some "unfortunate" incidents when messages were sent with inappropriate content of a confidential or abusive nature.

As a general rule, e-mail should be treated as per traditional paper communications. You should also note that you are responsible for the content and consequences of any mail sent!

Also, if you are considering forwarding your College e-mails to an external provider we strongly advise you seek guidance from the College Secretary, so as to avoid any possible breaches of the Data Protection Act. For further details see the Cloud Services: RHUL Code of Practice document at the back of these Session Notes.

20. Using the Global Address List with Outlook

The Global Address List (GAL) contains details of everyone on Campus with an e-mail address, and can be used to check and locate the correct e-mail address for new e-mails that you are sending to members of the College.

The Global Address List can be accessed in two ways:

By clicking on the To... buttons within a New Message Window.

By clicking on the Address Book button in the Find group at the right of the Home tab on Outlook’s Ribbon.

To use the Global Address List once the Select Names dialogue box is open with the Global Address List of staff and students at Royal Holloway displayed:
a. Click in the Search: panel at the top left of the dialogue box and enter the family name of the person you wish to locate.

b. Outlook jumps to the spot in the list that matches the name you have started to type.

c. Click on the correct name from the list.

d. You can check for further details of the name you have chosen by right-clicking over the person’s name and selecting Properties from the menu that appears.

e. When the Properties dialogue box displays you can check the person’s details before progressing.

f. When you have finished close the Properties dialogue box by clicking on OK.

g. If accessing the Global Address List from a Message window you can click on To:, Cc:, or Bcc: as appropriate to enter the e-mail address into the new message.

i. When finished close the Select Names dialogue box by clicking on OK.

Note: If you find that any of your own details are incorrect in the Global Address Book, they can be changed by accessing a form available from the Staff Telephone Directory web page, See Section 24 for details of how to make such changes.

21. Contact Groups (previously Known as Distribution Lists)

A distribution list, now termed Contact Group, is a collection of e-mail addresses which act as one e-mail address, so that when you send an e-mail to the Contact Group all recipients that make up the list receive a copy of the e-mail.

There are two types of distribution list:

A central Contact Group. This is created/updated centrally (usually by the IT Department) and displays within the Global Address List. This includes a number that are department-based and lists all students undertaking a particular course unit (based on Banner registrations).

If you wish to have a central distribution list created or modified please contact the IT Service Desk.

A personal Contact Group. This can be created/updated by the user.
Details on how to create personal Contact Groups can be obtained from Chris Horton (01784 41 4025, c.horton@rhul.ac.uk).

22. **Spam Control**

Spam is frequently referred to as unsolicited junk e-mail. As approximately 70% of incoming e-mails is spam the College employs a Spam filtering facility.

When spam that is addressed to you is received by the Spam filter it is placed into quarantine. Then, up to three times a week, an e-mail is sent to you listing all Spam messages that have been recently quarantined so that you can then decide whether you wish to access them.

From this e-mail you can:

a. Release the quarantined e-mail into your Inbox so that you can read it

b. Mark the quarantined e-mail as Not Junk to send the message to your Inbox. It will also notify the Spam Quarantine team that it was incorrectly marked as spam.

Note: To access many of the features available you will need to log on to the Spam facility. This uses your RHUL e-mail address as your username, and a password that you set within the Spam facility.

For details about using this facility and setting its password enter spam into the Keyword(s) text box of the FAQs panel on the IT Department homepage (see Section 2), or visit: http://www.rhul.ac.uk/it/faq/itfaqs/email/msspam.aspx

23. **Using Webmail/Outlook Web App**

Webmail enables you to access your College e-mails, Calendar, Tasks and Contacts when you are away from the College; all you need is an Internet connection.

Webmail can display in one of two formats:

The Full version, which appears very similar to Outlook, and incorporates a similar level of features.

Webmail will automatically display in this format when opened using a later versions of the mainstream browsers, e.g. Internet Explorer version 7 or later, Firefox version 3 or later, Chrome version 3 or later, or Safari version 3.1 or later.

The Light version, which is specifically designed to help those with visual disabilities, and provides less features than the Full version, with some of them used in a slightly different way to the Full version.

If using one of the 'less popular' browsers, e.g. Opera, Webmail will only display in this format.

Additionally, if you prefer this format you can set Webmail so that it always opens in this format, even when using a later mainstream browser.
Logging on to Webmail

b. Access the Internet in your normal way, and then open the webpage:
http://mail.rhul.ac.uk/

c. The Office 365 for staff login box will display.

d. In the Username: panel enter the username you normally use to log on to your PC on Campus, e.g. uvaa124

e. In the Password: panel type in the password you normally use to log on to your PC on Campus, remembering that this is case sensitive.

f. Click on Sign In.

Tips on using Webmail’s Full version

To display and hide subfolders
a. If necessary, click on the down-arrow to the left of the Folders heading to display all of the main folders.
b. Click on More at the bottom of the folder listing.

c. Click on the small right-facing triangle to the left of the folder whose subfolder(s) you wish to display.
d. The available subfolders will display below the folder.

e. Click on the required subfolder to display its content in the right-hand pane.

f. To hide the folders of an expanded folder click on the black down-facing arrow to the left of the main folder whose subfolder(s) you wish to hide.

Using Automatic Replies (Out of Office Reply)
Webmail enables you to set up, and turn on and off an Automatic Reply to your e-mails e.g. for when you are away from College:
a. Click on the Settings button (the Wheel/Cog button immediately to the left of the Help (question mark) button.
b. Select Automatic replies.

c. Under the Automatic replies heading, click on the Don’t send automatic replies or Send automatic replies option button as appropriate.
d. If you are setting up an Automatic Reply you can select a time period for the replies to be sent. To do this:
   (1) Ensure the Send automatic replies option button displays a check mark.
   (2) Click within the Send replies only during this time period check box so that it displays a tick mark.
   (3) Then set the required Start time and End time in the panels below.

e. In the text box immediately below the End time panel enter the message to be sent to members of College who e-mail you.

f. If you wish to additionally send a message to non-members of College who e-mail you:
   (1) Click on the Send automatic reply message to senders outside my organization check box so that it displays a tick mark.
   (2) Click on either the Send replies only to senders in my Contacts list or Send automatic replies to all external senders as appropriate.
   (3) In the text box immediately below these options enter the message to be sent to non-members of College who e-mail you.

g. When you have finished click on Save at the top of the window.

h. To return to your Inbox click on the Mail link at the top left of the window.

Tips on using Webmail’s Light Version

To Set Webmail to display using the Light version
It should be noted that you will be unable to view or access your OneDrive or Office 365 Sites when the Light version is enabled.
a. Ensure that Webmail is displaying.
b. Click on the Settings button (the Wheel/Cog button immediately to the left of the Help (question mark) button.
c. Select Options.
d. Click on the side-facing arrow to the left of the GENERAL heading in the left-hand panel to display its options.
e. Click on Outlook Web App version.
f. At the bottom of the list that displays click within the Use the light version of Outlook Web App check box so that it displays a tick mark.
g. Click on Save at the top of the window.
h. To enable the change log out of your e-mail account and restart your browser. When you logon again the Light version will display.

To display subfolders
   a. If displaying, click on the Click to view all folders link located below the main folders list.
   b. Click on the down-arrow in the panel that replaced the Click to view all folders link to display a list of all the subfolders available.
   c. Click on the subfolder you wish to display.
   d. Then click on the green arrow to the right of the panel to display the subfolder’s contents below the main folder listing.

Accessing your e-mails
   a. When using the Light Version only 20-25 e-mails per page are displayed.
   b. To navigate to further e-mails use the navigation buttons at the bottom right-hand side of the window.

Using Automatic Replies (Out of Office Reply) with the Light version Webmail enables you to set up, and turn on and off an Automatic Reply to your e-mails, e.g. for when you are away from College.

To do this:
   a. Click on Options at the top right of the window.
   b. Select Automatic Replies in the left-hand pane.
   c. Under the Automatic Replies heading, click on the Don’t send automatic replies or Send automatic replies option button as appropriate.
d. If you are setting up an Automatic Reply you can select a time period for the replies to be sent. To do this:
   (1) Click within the Send replies only during this time period: check box.
   (2) Then set the required Start time: and End time: in the panels below.

e. In the text box immediately below the End time: panel enter the message to be sent to those e-mailing you from within College.

f. If you wish to additionally send a message to non-members of College who e-mail you:
   (1) Click on the Send automatic reply message to External Senders check box so that it displays a tick mark.
   (2) Click on either the Send replies only to senders in my Contacts list or Send replies to anyone outside my organization as appropriate.
   (3) In the text box immediately below these options enter the message to be sent to non-members of College who e-mail you.

g. When you have finished click on Save in the blue band at the top of the window.

h. To return to your Inbox click on the Mail button at the top left of the window.

24. Using the College Telephone Directory

The College uses three different telephone number series, which means that when calling from outside the College the internal number for each series needs to be prefixed with a different number.

These prefixes are:
   3000 series numbers e.g. 01784 44 3063 need to be prefixed with 44
4000 series numbers e.g. 01784 41 4025 need to be prefixed with 41

6000 series numbers e.g. 01784 27 6140 need to be prefixed with 27

College telephone numbers can be found from the Global Address List or the College’s online Staff Telephone Directory.

The Staff Telephone Directory can be accessed in two ways:

By visiting: www.rhul.ac.uk/Restricted/Information-Services/directory/

From the College homepage:

a. Display the College home page at: http://www.rhul.ac.uk/
b. Click on the Staff button towards the top centre of the page to display the STAFF INTRANET page.
c. Point to the Tools and links link at the right of the top black band to display a menu of options.
d. Click on Use the staff directory at the bottom-left of the menu.

To find a telephone number using the Staff Directory

a. Click on the down-arrow to the right of the Select Department heading and choose the Department you require.
b. Click on Search to the right of the panel to display a list of the staff members in that department.

Or

a. Enter the family name, extension number or room number of the staff member whose telephone extension you require into the lower or enter Keyword (name, room or phone): panel.
b. Click on Search to the right of the panel.
c. Details of any staff member whose name, number or room number matches your search term will be displayed.

Correcting your own Details

If you find that any of your own details are incorrect in the Global Address Book or Staff Telephone Directory they can be changed by accessing a form available from the Staff Telephone Directory web page.

To do this:

a. Ensure that the Staff Telephone Directory: web page is displaying.
b. Perform a search to display your own details in the Telephone Directory.
c. Click on the Request Alteration button at the right of your entry.
d. The Update/Alter Your Details: form displays.
e. Complete the details you wish to amend, and then click on SubmitRequest.

25. Safe Surfing & E-mail Tips
It is important that you protect yourself whenever using the Internet or e-mail system. Therefore:

NEVER divulge your username, password, or any other personal details if requested in an e-mail – the College or a bank etc. would never request information from you in this way!

It should be remembered that these e-mails are purely designed to obtain the details to either empty your bank account or use your login details to hack systems!

Be wary of pop-up windows when browsing – these can hide viruses, trojan horses etc., so ensure you close them immediately by clicking on the window’s Close button. Do NOT click on any other button(s) provided, as they may download the virus etc.!

Never open unexpected e-mail attachments as they could contain viruses etc.! You might also wish to ignore unexpected e-mails for the same reason.

Additionally, be aware that a number of College members have recently received cold telephone calls attempting to sell antivirus software.

As such calls are highly unlikely to be from a genuine provider you should not undertake any instruction that they request/suggest, as this could do damage to your computer or laptop!
26. IT Skills – training documents available here:
https://intranet.royalholloway.ac.uk/staff/it-services/get-help-with-it/it-training.aspx
Royal Holloway’s
E-mail Guidelines
27. Royal Holloway E-mail Guidelines

Objectives:
We aim to use e-mail in a way that enhances internal and external College communication, providing a high level of service for our users and effective productivity for our own operations.
Guidelines on e-mails and the Law

This guidance is intended for every member of College staff who creates or receives e-mails as part of carrying out their contract of employment with the College.

Do remember that messages sent over the e-mail system can give rise to legal action against the College. Claims of defamation and breach of confidentiality or contract may arise from the misuse of the system. This applies to all users who send information/material to the College's e-mail and internet system via personal or private facilities.

When there is reasonable suspicion that the College computers or networks are being used to store, transmit or transfer data which breaches College regulations, the College's contractual obligation to third parties or UK law, the College will inspect or monitor activity and content to establish the existence of facts, to prevent or detect crime, to investigate or detect unauthorised use of telecommunication systems or, to secure, or as an inherent part of, effective system operation.

The College has the legal right, at any time, to inspect or monitor all data held on College computer equipment, and to inspect or monitor all e-mail and other electronic data entering, leaving, or within, the College network to ensure conformity with UK law.

The Data Protection Act permits people to see information that the College holds about them while the Freedom of Information Act gives people the right to access any other recorded information that the College holds, although there are some exemptions when these laws are overridden. It is advisable to work on the assumption that e-mails you create will be accessible to somebody.

Also worth noting:

E-mail messages are "creative works" and therefore copyrighted. The Copyright normally resides automatically with the sender or the employer by default, unless a contractual agreement to the contrary is in place. Thus for staff the copyright owner is the University whereas for students it is the sender. Messages posted to public lists do not lose copyright but the information may be archived or redistributed. Users should take care not to misquote, change or misattribute messages sent to a list.

Proprietary software and data must not be copied without the express permission of the copyright holders, except for the clearly-defined purpose of safety back-up.

Unauthorised access to a computer (sometimes called "hacking") or unauthorised modification to the contents of a computer (such as the deliberate introduction of viruses) are criminal offences punishable by unlimited fines and up to 5 years imprisonment.

Applicable Laws:

E-mail Good Practice:
E-mail is a relatively new medium and a variety of conventions have developed quickly, some more helpful than others. These guidelines aim to encourage good practice for RHUL staff.

Do:
Be aware of the legal guidelines if you use College e-mail for personal purposes
Respond promptly whenever possible, or use the out-of-office facility if you are absent for longer than a day or so
Always include an informative subject header
Keep your Autosignature short and relevant if you use one
Familiarise yourself with the “mass mailing” guidelines below
Keep e-mails short, and use unformatted text
Use reasonable formality - language more suited to face-to-face contact can offend or lead to misunderstanding, especially if you are not personally known to the recipient.
Be Legal, decent and honest

Don’t:
Don’t use e-mail for material which is strictly confidential (trials with secure e-mail are underway to facilitate use for confidential purposes)
Don’t include anything in an e-mail which will cause embarrassment if revealed - e-mails can and will be disclosed in the legal process
Please don’t take offence readily when less formal language is used in e-mail.
Do not send unsolicited, non work-related e-mail (spam).
Mark messages as urgent unless they really do require instant attention
Ever forward on chain letters
Ever forward virus alerts other (most are hoaxes) – get the professionals to do it officially.
Include personal or other abuse in messages

Student E-mail addresses:
All students are provided with a Royal Holloway address and mailbox. Official communications from the College to the student will use this mailbox and departments may require course-work submitted electronically to come from this address. Students may forward mail from the College address to a personal mailbox of their choice and personal mailboxes will be accessible from College systems where technically possible.

Responding Promptly & the 'Out of Office' Facility:
People generally anticipate a rapid response when sending e-mail, although this expectation may be unreasonable. To manage this expectation you should indicate when an e-mail enquiry will receive attention or use the out-of-office facility:
Aim to respond to e-mail within a working day either by dealing with the enquiry or by sending an acknowledgement
Set an ‘out-of-office’ message for absences of more than one day. The message should make clear how the correspondent might proceed with an urgent query in your absence
Nominate a colleague to read and respond to messages for staff who are away for long periods

Function-led e-mail addresses:
The anonymity of function-led e-mail addresses (eg any-enquiries@rhul.ac.uk) means that a prompt response mechanism is even more important than a personal mailbox – senders have
identified the address as a main point of contact, and the expectation of a rapid response or helpful acknowledgement is greater.

Incoming Junk/Spam Mail:
The College is making active efforts to control spam mail. Incoming mail passes through a spam trap which marks likely spam with a numerical score and a special addition to the subject heading. Mail recipients can then use mail filters to delete or move the messages away from the Inbox. In due course we intend to refuse to accept messages with a high spam score.

For 'Anti-Spam' Guidelines visit: http://rhul.ac.uk/information-services/computer-centre/facilities-and-services/service-overview- and-regulations/anti-spam.html

AutoSignatures:
Many staff adopt an AutoSignature to automatically add contact details to mail messages. Keep these short and to the point, and don't exceed five lines – include your name, job title and/or department, phone number, e-mail address and the College web address. E.g.:
Jo Bloggs
Departmental Administrator, Any Old Department
Royal Holloway, University of London
Tel : 01784 XXXXXX Fax : 01784 XXXXXX E-mail : j.bloggs@rhul.ac.uk
www.rhul.ac.uk

E-mail Circulation:
Before circulating information (mailing an identifiable group rather than a few individuals) please think carefully about the most effective channel of communication: Many staff are sensitive to receiving what they consider to be spam e-mail. Some guidelines follow for different categories of people.

Please restrict your use of College mailing lists to material which is of essential College relevance. Please don't repeat messages (and certainly don't send around a second message which is just an apology for a mistake in the first) and don't send objections about messages to the whole list. Please report** it to an administrator rather than starting an e-mail storm of complaints and counter-complaints.

In general attachments should not be circulated round mailing lists – please seek advice** about placing formatted information on the web/intranet and e-mailing a link to it rather than clogging mailboxes.

General information of interest to a majority of staff:
Use the Campus Intranet – send your information to Intranet@rhul.ac.uk, and it will be placed on the online message board within 24 hours.

The Intranet Message Board is restricted to campus access only and displays messages of interest to staff on a rolling basis in the order that they are submitted. The service is backed up
by a weekly digest e-mail to all staff, listing all messages posted online in the previous week. This is compiled and sent out by the Intranet Team on a Monday each week.

If you have very urgent or highly important information to share ask Intranet to mail your message to all staff. Intranet will send an e-mail to all staff on your behalf, but only in exceptional circumstances.
Bulletin Box - announcements of interest to all staff
Bulletin Box is exclusively used by the Principal to address all staff with the most urgent or important news and announcements. Bulletin Box messages are sent to all staff and circulation may also include all students.

Targeted information to reach a minority of staff:
There are numerous e-mail distribution lists to propagate information to individual offices or groups. These can be found in the Outlook Global Address List but you will find helpful information available from the Campus Classified page on the Intranet. No more than 4 lists should be aggregated in any one mailing.

The main circulation lists include:
- RH Dept Heads (includes The Head of each Academic department)
- RH Dept Contacts (includes a single point of contact in each Academic department, typically Department Administrators/Secretaries).
- RH Admin Heads (a single point of contact in each Academic Service or Administration department)
- RH Admin Contacts (a single point of contact in each Academic Service or Administration department, typically Department Administrators/Secretaries)
- All Staff (incl. all staff); RHUL staff (incl. all staff other than Central Administration)
- Administration (incl. those staff who are not on RHUL staff) - there is very limited access to these lists – Intranet is the main sender.

General information of interest to a majority of students: Intranet is the main sender and will send messages to all students in exceptional circumstances or for established routine communications of interest to the majority of students.

**Reporting - if in doubt - please seek advice from the Intranet Team – Intranet@rhul.ac.uk based in the External Relations Office.

These Guidelines can be accessed online at: http://www.rhul.ac.uk/it/tos/emailguidelines.aspx
Cloud Services
Royal Holloway’s Code of Practice
CLOUD SERVICES
RHUL
CODE OF PRACTICE

<table>
<thead>
<tr>
<th>Document Id</th>
<th>Cloud Services RHUL Code of Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sponsor</td>
<td>Laura Gibbs</td>
</tr>
<tr>
<td>Author</td>
<td>Nigel Rata</td>
</tr>
<tr>
<td>Date</td>
<td>October 2012</td>
</tr>
</tbody>
</table>
### Version Control Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>10/10/12</td>
<td>Initial draft for review</td>
</tr>
<tr>
<td>1.1</td>
<td>01/13</td>
<td>Initial draft published</td>
</tr>
<tr>
<td>1.2</td>
<td>13/02/13</td>
<td>Updated post comments from ITUAG</td>
</tr>
</tbody>
</table>

### Document Approval

<table>
<thead>
<tr>
<th>Name</th>
<th>Approval Signature</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITUAG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction

The University is currently considering its policy regarding the use of ‘cloud computing services’.

Until this policy is published, cloud computing services should not be used for processing data which is:

i. Sensitive personal information as defined by the Data Protection Act (DPA) 1998; ii. Confidential to the University or a third party;
iii. Of such criticality that functions or operations would be disrupted should it be unavailable lost or become corrupted;
iv. Valuable intellectual property of the University

This guidance document gives some background to the above.

As a member of RHUL you are responsible and liable for the data that you handle and not your line manager or Royal Holloway University of London (RHUL) itself. Any member of the University who is considering or is already using cloud storage for University information assets needs to be aware of the risks posed by using these services. This code of practice is intended to make you aware of the risks and give specific circumstances when cloud based services should not be used. It is informed by the University Information Security Policy and relevant sub-policies. This guidance has been produced to help staff make decisions when considering the use of cloud based services.

RHUL IT Services provides a number of services which could be used as an alternative to taking a cloud based service. These include:

- Webdav access to y-drive from most mobile phones and tablets
- VPN for remote access to college resources
- Webmail/Activesync for access to college e-mail as well as support for all mobile device platforms.
- Coming soon – remote access to popular apps in our Remote Desktop Services solution.
For the last 5 years the IT strategy of RHUL has been to consume cloud services on an enterprise scale where appropriate. This is done with the appropriate due diligence (financial, contractual, security and legal etc).

RHUL students have been on the Microsoft Cloud based email platform Live@Edu for the last 3 years. In the last 3 months RHUL is consuming a cloud based spam protection tool for all incoming e-mail. This guidance, although pertinent to the enterprise agreements, is focused however on ad-hoc arrangements made between individual and/or groups of staff and cloud service providers.

**Summary of the guidance:**

Do not store data on ad-hoc cloud services that:

- Contains sensitive personal information as defined by the Data Protection Act (DPA) 1998;
- Is confidential to the University or a third party
- Of such criticality that functions or operations would be disrupted should it be unavailable lost or become corrupted
- Is valuable intellectual property of the University

**Cloud Storage and Service providers**

For the purpose of this document, cloud storage can be defined as any storage solution which stores University information assets to an online storage facility not provided by the RHUL.

Cloud-based or “capacity-based” storage is a popular solution for storing data. Cloud services are provided by large and trusted technology companies including:

<table>
<thead>
<tr>
<th>Cloud Service Provider</th>
<th>Cloud Storage Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>Amazon EC2</td>
</tr>
<tr>
<td>Apple</td>
<td>iDisk, iCloud</td>
</tr>
<tr>
<td>Dropbox.Inc</td>
<td>Dropbox</td>
</tr>
<tr>
<td>Google</td>
<td>Google Docs, Google Apps, GDrive</td>
</tr>
<tr>
<td>Microsoft</td>
<td>SkyDrive, Office 365, Azure</td>
</tr>
</tbody>
</table>
N.B this is not an exhaustive list. Many Web 2.0 or social media applications and services often have storage capability.

Whilst these services are undoubtedly attractive, offering excellent features that are easy to use often at low cost, they bring with them a series of risks to the University and its information assets which must be considered.

**Legislation and Information Assets**

There are many situations where the data used by members of the University requires stringent protection which must satisfy both University regulations and government legislation. Those involved in medical research, for example, will be aware that there are obligations to protect patient confidentiality. The Information Security Policy and other policies e.g. data protection etc. provides more guidance on these matters. If there is any doubt regarding the classification of data you must seek advice from the College Secretary.

**Service Providers, Contractual Agreements and Risk**

All data generated as part of your duties as a member of the University belongs to the RHUL and should be managed in line with college guidance. If such data is stored on facilities provided by RHUL central IT it is protected and in compliance with the policy. Using a cloud-based storage system will put you at risk of contravening college policy or the law of the land as there are very few guarantees provided by cloud storage services. Using cloud-based storage encumbers you with a high dependency on the security of the service provider and there is often very little recourse in the event of a security breach.

This is highlighted in an extract from the Master Subscription Agreement of a cloud storage provider:

```
“...salesforce.com shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any Customer Data.” 03/04/2012
http://www.salesforce.com/company/legal/agreements.jsp
```
Ownership

As previously stated, all data generated in carrying out your duties belongs to the University. Using cloud storage may require you to transfer ownership of University data which you may not be eligible to do. The following extract is from the terms and conditions of the popular cloud storage provider Dropbox:

“If you are using the Services on behalf of an organization, you are agreeing to these Terms for that organization and promising that you have the authority to bind that organization to these terms. In that case, “you” and “your” will refer to that organization...”

“You may use the Services only if you have the power to form a contract with Dropbox ....” 03/04/2012
https://www.dropbox.com/terms#terms

Data Protection

Data protection is a complex area but its requirements apply to all members of the University. The College Secretary is the Data Controller for RHUL and may be liable for any data breach which results from the use of cloud storage. Whilst all principles of the Data Protection Act are relevant, in relation to cloud storage particular attention should be paid to Principle 8 which refers to sending personal data outside the European Economic Area.

Principle 8 states:

“Personal data shall not be transferred to a country or territory outside the EEA 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 data.”

Many of the popular cloud storage solutions store data on servers based in the United States. Unless they have signed up to the Safe Harbor scheme they cannot be considered to offer adequate level of protection. The following is an example from the Microsoft Azure .NET Services Platform Terms of Use:
“Personal information collected through the Services may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries or service providers maintain facilities.”

Current debate suggests that in practice the Safe Harbor scheme offers no guarantee of compliance to the EU Data Protection Directive due to the far reaching implications of the USA Patriot Act.

Data Management

Data which has been generated as part of the carrying out your role at the University must be managed appropriately. For example, data may need to be deleted after a certain period for compliance purposes. It could be a legal requirement to demonstrate that this data has been permanently deleted and to provide supporting evidence. Clearly, this is likely to be very difficult to achieve if data has been stored in the cloud. It would also be difficult to audit exactly where the data resides, if required to do so.

Data Access

At times, data generated as part of your role may need to be accessed by colleagues or authorised members. Cloud storage solutions do not integrate with the University’s authentication systems so would require all those who require access to the data to register for external accounts. If the holder of the account where the data resides is unavailable for whatever reason it may not be possible to gain timely access to the data. In some circumstances it may mean that the data cannot be accessed for long periods or may be permanently lost.

Reliability and Availability

Using cloud-based storage encumbers members with a dependency on the stability and speed of network connections. Such a connection to a cloud storage server cannot be guaranteed due to various processes from PCs/tablets/smartphones to the cloud storage servers. Depending on the features offered by the cloud storage service, it is likely that there will be a period when the data or the latest version of the data is not accessible. In the event of downtime, there is often very limited recourse.
This is highlighted both in the Amazon Web Services Customer Agreement and the Google Apps Premier Edition UK Terms and Conditions.

"[We] do not warrant that the service offerings will function as described, will be uninterrupted or error free, or free of harmful components, or that the data you store within the service offerings will be secure or not otherwise lost or damaged..." 03/04/2012 http://aws.amazon.com/agreement/

"Google and partners do not warrant that i) Google services will meet your requirements...ii) Google services will be uninterrupted, timely, secure or error free or reliable... iii) The results that may be obtained from the use of Google services will be accurate or reliable iv) any errors in the software will be corrected." 03/04/2012 http://www.google.com/apps/intl/en-GB/terms/user_terms.html

Company Viability

Regardless of the legal constraints, the long-term viability of the cloud storage company must be taken into consideration. In recent years, dozens of cloud storage companies have ceased trading after being unable to maintain commercial viability. Some of these companies have offered a means of transferring data from the cloud back to local storage or another cloud provider which entail modifying the level of complexity and varying periods of notice. As well as complete closure, other cloud storage companies have been forced to reduce their storage quotas and to introduce stricter fair use policies or increase prices in order to stay commercially viable.
Acknowledgements:

University of Liverpool and University of Leeds.
Royal Holloway’s Password Policy
Password Policy
<table>
<thead>
<tr>
<th>Title</th>
<th>Password Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document ID</td>
<td>Password Policy</td>
</tr>
<tr>
<td>Current Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Sponsor</td>
<td>Laura Gibbs</td>
</tr>
<tr>
<td>Author</td>
<td>Dave Cobb</td>
</tr>
<tr>
<td>Date</td>
<td>13/02/2012</td>
</tr>
</tbody>
</table>

© Copyright Royal Holloway and Bedford New College. The copyright in this document is vested in Royal Holloway and Bedford New College which may also be referred to as Royal Holloway, University of London. The contents of the document must not be reproduced wholly or in part, used or disclosed without prior written permission.
Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>30/11/11</td>
<td>Draft for review</td>
</tr>
<tr>
<td>1.1</td>
<td>13/02/2013</td>
<td>Annual update and review</td>
</tr>
</tbody>
</table>

Document Distribution

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank Briggs</td>
<td>Head of Service Delivery</td>
<td>Document Review</td>
</tr>
<tr>
<td>Nigel Rata</td>
<td>IT Infrastructure Manager</td>
<td>Document Review</td>
</tr>
<tr>
<td>Laura Gibbs</td>
<td>Deputy Registrar and CIO</td>
<td>Document Review &amp; Approval</td>
</tr>
<tr>
<td>Judith Croker</td>
<td>Head of IT Development</td>
<td>Document Review</td>
</tr>
<tr>
<td>Sarah Honeycombe</td>
<td>Communications Assistant &amp; Student Liaison</td>
<td>Document Review</td>
</tr>
<tr>
<td>ITUAG</td>
<td>Various</td>
<td>Document Review &amp; Approval</td>
</tr>
</tbody>
</table>

Document Approval

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITUAG</td>
<td>23rd February 2012</td>
</tr>
</tbody>
</table>

Contents

Introduction .................................................................................................................................................. 3
Objectives ................................................................................................................................................... 3
Scope .......................................................................................................................................................... 4
Password Policy ......................................................................................................................................... 4

IT Services Internal Use Only

Password Policy
Introduction

Secure passwords, in both construction and safeguarding, are critical elements of digital security. Poorly designed or protected ones can lead to an entire network being compromised and personal data being maliciously accessed. All users at Royal Holloway are expected to abide by the guidelines set out in this policy document.

Objectives
1. Define password standards for end users and system administrators
2. Safeguard user data and data users hold responsibility for
3. Maintain confidence of external organisations in our data safeguarding processes
4. Reduce the possibility and implications of identity theft
5. Avoid unnecessary or complex security procedures by considering the user experience

Scope

This policy is applicable to all users who hold any kind of password authenticated access to any system at Royal Holloway, University of London, on its network or that is otherwise associated with Royal Holloway (such as passwords from systems hosted outside RHUL).

Password Policy

Overview

Passwords are mainly for a user’s personal account only and must not be shared or disclosed to anyone. The scope of this policy also includes system passwords that are non-person specific and relate to roles. It is an offence under the Computer Misuse Act (1990) to access or attempt to gain access to a computer system or material to which one is not entitled. It is also a breach of this policy for any user to misuse their, or another’s, password. If any such misuse results in a user knowingly elevating their system privileges above their assigned level this will be considered an act of gross misconduct.

All user-level and system-level passwords (i.e. basic user, super user, domain administrator) should conform to the guidelines below. In cases where technology prevents this, each exception will be managed and noted on an individual basis. This policy will outline the process by which these exceptions are agreed and managed.

Guidelines

Most users will only have a small number of passwords whilst at Royal Holloway as, strategically; services are implemented with a single-sign-on (SSO) system using a college username and password where possible. Notable exceptions include Turnitin native, MyView (staff payment system) and Upay (the RCS College card top-up system). This makes these guidelines easy to follow for the vast majority of users.
Construction

All passwords must:

- be at least eight characters
- include at least three different types of character from the following
  - uppercase (A-Z)
  - lowercase (a-z)
  - numeric (0-9)
  - special (! @ # £ $ % ^ & * ( ) _ ‐ + = | ~ \ [ ] : ; “ < > , . / `)

All passwords should:

- not be a word in any language, slang, jargon, etc.
- not be based on personal information (names, fantasy characters, pets, etc.)
- not use computer or Royal Holloway related terms
- not use addresses or phone numbers
- not contain common patterns (e.g. qwerty), repeating patterns (e.g. 12341234) or reflected patterns (e.g. 12344321)
- be based on something memorable

Disclosure

Under no circumstances should any user reveal their password in any way to anyone. Users should never store a password on any computer system unless it is heavily encrypted and ‘remember password’ features should not be used on any shared devices.

If an account or password is suspected to have been compromised, the incident must be reported to the IT Service Desk immediately.

Creating and changing passwords

When a new password is set up by anyone other than the user (typically when it is first created or has been forgotten), wherever possible, the new password will be communicated without anyone else becoming aware of it. Where this is not possible, the user will be required or at least encouraged to change their password immediately.

Users can change their SSO password at any time from a Royal Holloway computer or by visiting passwordmanager.rhul.ac.uk.

Account locking
If more than 20 attempts are made in the space of five minutes to access an account then a ten minute lockout will ensue. The account can be reactivated by contacting the IT Service Desk or waiting for the lockout to expire.

If a user manages to lock themselves out of their account by forgetting the password, the IT Service Desk will only unlock the account once the user has proven their identity.

**System and Application administration standards**

System and application administrators hold responsibility for implementing this policy and should follow the following additional guidelines wherever possible:

- Password complexity should be enabled to prevent the use of dictionary passwords
- Sharing of system-level accounts should not be used
- If a system provides intruder lockout or break-in evasion features these should be enabled
- Passwords must be stored in an encrypted fashion and password databases protected
- No blank or default passwords are allowed to be used on any system

These administrators include IT Services staff, super users at Royal Holloway and staff with IT responsibility in departments.

1 IT Service Desk: #4321, itservicedesk@rhul.ac.uk

**System and Application procurement and development standards**

When purchasing or developing systems that rely on password authentication there are a number of minimum standards that must be met:

- Authentication must be for individuals not groups
- Passwords must be stored in an encrypted format
- Provide the capability for role management so one user can subsume the responsibilities of another without their password
**Enforcement**

Failure to comply with this policy document may result in disciplinary action. Compliance is essential to avoid data theft and unauthorised system access.

**Exceptions**

Whilst this policy is designed to affect all instances of passwords use at Royal Holloway, there are always exceptions. Users of applications that, for whatever reason, do not conform to these guidelines will be issued with additional information as required.

For systems that wish to be exempt or deviate from this policy - approval must be given by the CIO. The decision and supporting material will by collated with this policy as a record of the process (however these details will not be distributed or published).
Appendices

Appendix I – Password construction tips

Some handy hints for choosing and securing your password:

- Include similar looking substitutions, such as the number zero for the letter 'O' or '$' for the letter 'S'.
- Include phonetic replacements, such as 'Luv 2 LaF' for 'Love to Laugh'.
- Choose two objects from a picture that you’ll always remember. For example: a drawing at your grandparent’s house, the illustration from a children’s book, a painting at an art museum, etc.
- Choose two terms from a memorable purchase: bluev6 (first car), thinibm (first computer), gold3crt (engagement ring), 7ftgrand (piano), pinedoor (first house).
- Look through a catalogue and choose terms based on something you see.
- Look up a random article on Wikipedia and choose a word found or related to a word you find in the article.
- Separate your two words with symbols and numbers: pine&1&door, kit!2!cat, etc.
- Modify the password for each site: In theory, the most secure password strategy is to use a completely different password for each system. In practice, this means you’ll have to write them down. By choosing a secure password and modifying it based on where it will be used, you can keep a slightly higher level of security. Here are some examples showing how they were created:
  - blue.Mv6 for Amazon.com – blue and v6 from first car. M from the second letter in site name.
  - blue.Av6 for SAP logon – same as above.
  - thin!5!ibm for Amazon.com – thin and ibm from first computer. 5 from the number of letters in the site name.
Acknowledgements:

University of Liverpool and University of Leeds.