Rooks Heath College

ICT Policy

Introduction

This policy replaces any previous policy and follows the DfE regulations.
In line with the College's Equal Opportunities and Special Educational Needs policies, we aim to give all students equal opportunities to take part in all aspects of College life, as far as is appropriate, practicable and compatible with giving regard to health and safety and the efficient education of other students.
This policy takes account of the Government's aim for children to have the support they need under Every Child Matters:

- to be healthy
- to stay safe
- to enjoy and achieve
- to make a positive contribution
- to achieve economic well-being

The policy will follow the five principles of the Children's Plan:

- to support parents and families
- to allow children to reach their full potential
- to enable children to enjoy their childhood whilst preparing for adult life
- to provide services in response to children and family needs
- to use preventative measures to help students avoid the possibility of failure

This policy is based upon the College's commitment to the development and maintenance of good behaviour and a positive and inclusive ethos for all members of the College community.

Revised Edition: May 2017
Ratified by Governors**:** 5th July 2017
To be reviewed every 3 years

Foreword

Rooks Heath College is a mixed 11 to 18 multicultural comprehensive in the London Borough of Harrow. This policy is formulated by the Associate Headteacher, in consultation with staff, particularly ICT & Computing staff, and is monitored by other members of the College's Leadership and Management Group. The policy is subject to review every 3 years by the College's Leadership and Management Group and is subject to approval by the governors of the College.

Due to the ongoing advancement of ICT, procedures outlined in this policy may change before the policy is due for review.

Aims of this policy

- To ensure that the College's digital resources are used safely and in a professional manner
- To safeguard students and staff from ICT related issues and ensure that RHC community is an e-safe community

Introduction

This policy is based on government guidance on the acceptable use of ICT systems. It has been agreed by the senior management and approved by the governors. The policy will be implemented by all staff and students and will be monitored by the network manager and Associate Headteacher

Due to the nature of the internet, social media and advancement in digital technology, it is accepted that there is no technical solution that can consistently guarantee to prevent the misuse of ICT, cyber-bullying or the access to unwanted internet material. The College will not accept liability for the material accessed or any consequences of Internet access thereof.

However, such circumstances will be carefully monitored, recorded and dealt with in accordance with this policy. The College treats e-safety as an important aspect for education and encourages parental involvement in the implementation of this policy. *Securus*, the College's monitoring system, is used to protect students and staff from the risks associated with the use of the internet and ICT systems.

Why ICT is important for students and staff

The purpose of ICT and Internet use is to raise standards, promote student achievement, to support the professional work of staff and to enhance the College's management administration systems. ICT and the internet is part of the statutory curriculum and a necessary tool for staff and students. The internet enables access to world-wide resources and access to the College's Managed Learning Environment (MLE). The College's internet access is expressly for student and staff use for educational purposes and includes appropriate filtering and monitoring (by LGfL and the College). If staff or students discover unsuitable sites, the URL (website address), content is to be reported to the ICT Support Team for these URLs to be immediately blocked.

Passwords

Access to College ICT systems may only be made with the user's authorised username and password, which must not be given to any other person. Passwords for all users will be reasonably complex and will be at least alpha numeric and subject to at least annual change.

Use of digital and video images on the website and the management of College's website and MLE

The point of contact on the website will be the College address, email and telephone number. No personal or social media information of students, staff or contractors will be published by Rooks Heath on any website.

Parental permission is obtained for using photographs of students.

The Associate Headteacher and Business Manager will oversee and authorise the website's content and check the suitability of any images used. Uploading of information to the website will be restricted to staff members nominated by the Associate Headteacher, the Director of Business or the Assistant Director of Business. Digital images of students and staff will be stored in the secure area of the College network without the written permission of the person or patent/carer. Parents are required to give consent for photographs to be used for publicity.

Staff with responsibility for managing and accessing personal data in the College's Management Information Systems or the MLE, will comply with the following conditions:

1. The data is to be used only for educational purposes or the business function of the Academy.
2. Personal data is to be shared only with those who need the information to discharge a statutory education function and will not be sent outside of the Academy without explicit approval from the Associate Headteacher or the Director of Business.
3. Only authorised users may access the system and they must never share their login details with anyone.
4. Management of Canvas usernames and passwords is the responsibility of the authorised system manager, under the direction of the MLE administrator in the College.
5. Any confidential or personal data will be handled with strict confidentiality and any printed material, that has personal details, will be shredded when not required.
6. Temporary data sets, mainly from SIMS or systems that hold personal information, will be deleted as soon as possible, usually on a daily basis. It is the responsibility of the user to ensure that data sets are secure and cannot be misused or misplaced. Data taken off site must be encrypted.
7. Permanent data will be deleted from all College systems and devices by individual staff members and staff in charge of data sets, such as the Network, Data and Exams Managers, will do so in line with current regulations. In cases when there is no further need to keep such data, this will be deleted sooner. We recognise that the regulations are to change soon and we will comply with these changes as soon as they are clear.

Failure to comply with these conditions will be considered as Misconduct and potentially Gross Misconduct.

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. The College, in conjunction with LGfL,

will block social networking sites. Forums set up within the College's MLE will be acceptable.

It is the responsibility of Parent/Carers to manage and control what is published by their child at home on social media and the internet.

How will emails be managed?

Students will use the LGfL secure email system. Students are told to immediately tell a teacher if they receive offensive email and not to reveal details of themselves or others in email communication. This includes information such as their address or telephone number. They are told not to arrange to meet anyone. Emails sent to an external organisation should be written as carefully as a letter written on College headed notepaper.

Staff will use the internal exchange or LGfL email system but the MLE (Canvas) is also increasingly being used. The College's email disclaimer is expected to be added to emails sent to addresses external to the College.

No member of staff or student is allowed to send any personal information, relating to others, outside of the College without the explicit approval of the Associate Headteacher or the Director of Business.

Mobile devices

Mobile phones (or similar mobile devices that can access the internet, record and transmit text, sound, images etc.) will not be used during lessons or formal College time unless expressly agreed by the class teacher for specific one-off purposes. The recording and sending of abusive or inappropriate text messages, sounds or images (still or moving) is forbidden. The use of recording technologies by staff is only permitted to facilitate students learning.

Where College mobile phones have multiple users, the usage will be closely monitored. Users will sign for these and take full responsibility for these whilst in their care. Pin codes for mobile phones will be kept secure. At the end of the loan all data will be deleted from the mobile phone. The Associate Headteacher will monitor this. Any apps downloaded for the activity will be deleted. *See also Appendix E.*

Internet access

Students and staff must read the guidelines for acceptable use of digital devices and agree to abide by the 'Acceptable use of digital and ICT devices' policy on each occasion they use the College's IT systems before access is given. *(See Appendix A).* Parents also sign a Consent form when their child joins the College agreeing to their use of the internet and other ICT facilities. This information is stored in SIMS and the hard copy filed with the student's records. The Network manager is responsible for ensuring that only students who have parental consent have access to the internet.

Filtering internet access

Blocking strategies by LGfL and the College help prevent access to a list of unsuitable sites or newsgroups. The ICT Support Team will maintain and update the blocking list as new sites appear. The Associate Headteacher, Director of Business and the Assistant Director of Business will monitor internet sites visited by individual users, along with their use of our ICT systems, with the

aid of *Securus*. All sites are blocked until LGfL receive a request to allow the site to be viewed. Only sites that are then approved will be available.

Dealing with Inappropriate Use of College ICT Equipment

Staff and students are expected to follow any guidance contained within this policy and ICT support staff. Users are expected to use the systems safely, particularly when accessing and using sensitive data. ICT support staff are expected to keep the system as safe and secure as possible by using appropriate software, such as anti-virus programs. *See also the Data Protection policy*.

Students

Responsibility for handling student incidents is carried out by the Associate Headteacher, Director of Business and the Assistant Director of Business. They monitor Securus between them on a daily basis. They either deal with any cases discovered or delegate to the IT Technical staff or the DoL, depending on the severity of the incident and consequence needed, An incident log of banned students is kept and monitored by the IT Technical staff, who will contact the Associate Headteacher or a member of the Pastoral Team if necessary. See also the Behaviour for Learning policy.

Staff

Staff who use College equipment inappropriately will be dealt with using the procedures outlined in the College's HR policy. It will be deemed Misconduct or Gross Misconduct, depending on the level of failure or degree of abuse. Responsibility for dealing with staff misuse will be by the Headteacher, or the Associate Headteacher in his absence. A list of staff offenders is kept by the Associate Headteacher. See also the HR policy.

Governors

Access to College systems by members of the Governing Body is very limited.

Regulation of chat rooms, newsgroups, forums and RSS feeds

Students will only be allowed access to approved chat rooms, newsgroups, forums and RSS feeds with approval of the Associate Headteacher in consultation with the Network Manager. RSS feeds may be available through the College MLE provided staff can demonstrate an educational benefit for using them.

Security of the ICT system

The College's ICT Support Team will be responsible for installation and regular updating of virus protection. Use of personal portable storage media such as USB memory sticks, DVDs, CD-ROMs and other portable storage devices are reviewed on an as and when basis. *See also below.* Access to files are automatically scanned in 'real time' and reports are sent to IT Support. *See also the Rooks Heath Critical Incident* and *Data Protection policies.*

Portable devices

Generally speaking, personal portable devices cannot be connected to the College system. However, exceptions are made for certain subject areas, such as Photography where files are very large and for certain cases at the discretion of the Associate Headteacher in consultation

with senior ICT Support Staff.

Software

Only software approved by the College will be installed on college computers and only ICT support staff have the necessary permissions to do this. Unlicensed and Open Source software cannot be used on the College's system. Only the Network manager can authorise software installation by the ICT support team.

Backups

The Network manager is responsible for encrypted backups of all College systems which are made and kept off site, currently using Gridstore.

Loss of ICT Equipment

In the event of complete loss of the College's ICT equipment, the Support Team will be responsible for getting the systems working again. Cloud based services will also cause downtime if these services fail. This is likely to take at least 6 weeks. The costs at the time of writing this policy are indicated below:

Item	Quantity in school	Cost per item	Total Cost	Life cycle in years
Computers	550	£420	£231,000	6
Projectors	68	£800	£54,400	3
Laptops	50	£420	£21,000	4
IWB	68	£1,400	£95,200	5
AIO IWB	2	£2,600	£5,200	4
Colour Printers	35	£500	£17,500	5
BW Printers	30	£250	£7,500	5
Speakers	71	£80	£5,680	5
Servers	5	£4,400	£22,000	3
SAN	1	£20,000	£20,000	3
UPS	2	£1,500	£3,000	3
KVM	2	£1,500	£3,000	4
Switches	35	£400	£14,000	6
Wireless Point	50	£400	£20,000	5
Bulbs	67	£260	£17,420	3
Monitors	660	£70	£46,200	5
Tablets	70	£400	£28,000	2
Wireless server	1	£2,500	£2,500	5
		Total	**£643,100**	

Protecting Data

Staff are permitted to take student data off site as long as they have a genuine need to do so. This data will be encrypted or password protected and deleted at the earliest opportunity. Where pages have been printed, these will be shredded at the earliest opportunity. Data taken off site will be encrypted using tools provided by the Network manager.

Although encryption is recommended for protecting data in the UK, some countries ban the use of encrypted data. When travelling to countries as part of an educational visit, where encryption is not permitted, the College will check current restrictions with encryption software or encrypted data before leaving the UK. Removal of any encryption software and encrypted data from laptops or mobile devices will need to take place or application for the appropriate licence well in advance before leaving the UK.

Some countries with encryption restrictions are: China, Morocco, Russia, Cuba, Ivory Coast, Iran, and Iraq.

Introduction of the policy to students

Students will be required to accept the guidelines for acceptable use of digital devices every time they log onto a College computer, laptop or other equipment. They are not able to log on unless they agree to the terms set out on the log on screen.

A module on responsible internet use is included in the Computing curriculum covering both College and home use. This module will include cyber-bullying and e-safety and are part of the Computing and PSE departments' schemes of work. Also covered is password awareness.

Informing staff

All staff including teachers, classroom assistants, supply staff and support staff, will be required to accept the terms of the Acceptable Use of Digital Devices Policy before using any ICT resource. Staff will be made aware that internet traffic is monitored and traced to the individual user and machine and that discretion and professional conduct is essential. Failure to follow the Policy will result in disciplinary action. Reminders are sent to staff at regular intervals. Visitors are not usually allowed access to College ICT systems, although limited access is given to some trainee teachers, at the discretion of the Associate Headteacher.

Informing Parents/Carers

Parents'/Carers attention will be drawn to this policy on the College website. Parents will be required to read the guidelines for acceptable use of the College's ICT systems with their child and sign the agreement. A partnership approach with parents will be encouraged. Information on 'cyber-bullying', 'safe use of the internet' will be published on the College's website and MLE *(Canvas)*. A copy of this policy can be found on the Rooks Heath website. Further information is given to parents/carers on admission to the College, as part of the induction process.

Sanctions for the misuse of the internet facilities and digital devices

There may be a temporary removal of access to the College network for a fixed or unlimited period if students misuse ICT facilities. There may be occasions when the police may need to be contacted. Depending on the nature of the incident, sanctions for misuse or irresponsible use include bans from using the College's ICT facilities, seclusions and exclusions in accordance

with the College's Behaviour for Learning policy. Parents will be charged the cost of replacement that is needed because of any wilful damage by their child.

Staff are expected to have high standards of ICT use and will face disciplinary action if they abuse the rules concerning the use of this. This includes the use *anywhere* they use College ICT equipment. *Securus* monitors staff use of College ICT equipment, even offsite.

Leavers

When students or staff leav the College, their accounts will disabled as soon as is practicable. In the case of users facing disciplinary action, this will be immediate. Data will usually be kept for a minimum of 7 years. This data is securely kept by ICT Support and is accessible to the Headteacher, Associate Headteacher or Director of Business if required.

Extended Assurance

The College's ICT systems and relevant policies are checked at regular intervals.

The College follows the requirements, as set out by EFA in the Academies Financial Handbook, to undergo a process of review and scrutiny of processes and governance of its ICT systems and procedures. This is largely done by the Associate Headteacher, Director of Business, the Assistant Director of Business, Head of Computing and the Network manager. The ICT systems and processes are subject to review by the College's auditors according to the work programme agreed by Governors and once a year at the annual audit.
The Associate Headteacher gives regular reports and, over time analysis, to the Headteacher of misuse of the ICT systems by students. Staff incidents are reported immediately they are discovered.

Appendixes

Appendix A

Acceptable Use Contract is the College's Acceptable Use of Digital and ICT Devices contracts for both students and staff.

Appendix B

Student Laptop Agreement Form is the College's form that is completed by students if they have occasion to use a College Laptop or other digital device.

Appendix C

Incident log form is the College's incident log form. This will also be logged in the College's BfL system.

Appendix D

Acceptable use of Digital and ICT devices – Staff contract is the form staff sign before they can access the College's digital devices, including College mobile phones.

Appendix E

Acceptable use of Mobile Phones issued by the College outlines the expectations of staff who use College mobile phones.

Appendix F

OSA Mobile Phone Log is a record of the use made of the College mobile phone used for Off Site Activities

Appendix A

Acceptable Use Policy

This is valid for ALL users of the system.

This Acceptable Use Policy will help protect all users by clearly stating what is acceptable and what is not.

1. Anyone using RHC ICT systems will adhere to the ICT policy or face relevant disciplinary measures..

2. Computer access may only be made with the user's authorised username and password, which must not be given to any other person.

3. College computer and Internet use must be appropriate to a pupil's education or to staff professional activity.

4. Copyright and intellectual property rights must be respected.

5. Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. Communications by e-mail are not secure and as such, should be regarded as public property.

6. Pupils must never give out personal details such as name, address, age or telephone number. Any unsuitable communications received must be reported to a member of staff immediately.

7. Use of the network to access or send inappropriate materials such as pornographic, prejudicial, racist or offensive material is forbidden. Anonymous messages and chain letters must not be sent.

8. Staff should abide by the College policy on data protection when dealing with sensitive data.

9. The attempted use of proxy servers to bypass College internet restrictions is not allowed.

10. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

11. The integrity and security of ICT systems must not be compromised. Any form of hacking or accessing restricted files will not be tolerated.

Irresponsible use may result in being banned from the internet or loss of access to all College computer systems.

The College will exercise its right to monitor the use of computer systems, including the monitoring of internet use, interception of e-mails and the deletion of inappropriate materials at all times. In circumstances where the College believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the College reserves the right to inform appropriate authorities and provide documentary evidence. Internal procedures also follow – see elsewhere in this policy.

Appendix B Student Laptop Agreement Form

Introduction.
This agreement has been drawn up to set the conditions by which a student may have personal use of a College laptop computer, be it supplied directly by the College, or via any other laptop funding scheme. The Student Laptop Agreement Form is set out to inform all of the conditions under which they may have the use of a College laptop computer, and is intended to guide and protect both the student and the College.

In order to effectively administer all of its computer systems against attack by viruses, spyware and hackers, the College reserves the right to scan, review and delete any files that may be held on its computer systems, including laptops. This may at times necessitate the monitoring of an individuals computer and/or internet activity. In any circumstances, personal privacy and confidentiality will be strictly observed at all times.

Student Laptop Acceptable Use General Statement.
The agreed conditions under which a Rooks Heath laptop computer is allocated to a student use by Rooks Heath College include, but are not limited to, the following;

- I accept personal responsibility for all use of the Laptop Computer issued to me.
- Every care and consideration will be made by myself to look after and protect the laptop which has been supplied to me for my personal educational use by the College.
- Laptop use should be appropriate to personal education or staff professional activity.
- Computer and Internet access should only be made through my own login, which should not be made available to any other person.
- I understand that as the laptop will regularly be attached to the College's computer network, every care must be taken to prevent it becoming infected with any computer viruses or other malicious software which it might then pass on. To this end, I will undertake to;
    1. Regularly update the definitions utilised by the laptop's pre-installed Anti-Virus software and Anti-Spyware applications, if applicable. (see point 3)
    2. Regularly perform a Windows Update to keep my laptop protected with the latest patches, fixes and software updates. (see point 3)
    3. Where it is not possible to undertake points 1 and 2 myself, I will regularly return my laptop to the ICT Support team so that they may undertake the required operations for me.
- In any case, when requested, I will return the laptop to the ICT Support staff so that a general health check and service can be undertaken upon it.
- I will immediately report any problems or concerns found with the laptop to the ICT Support Team.
- No files shall be downloaded from the Internet unless directed by the teacher in charge of the lesson.
- Any special conditions listed below will be observed and strictly adhered to.
- Use of the laptop to access inappropriate material such as pornographic, racist or offensive material is strictly forbidden.

Special Conditions for Student:
I understand that laptop computers are extremely vulnerable to theft and special care must be taken to keep them safe. In particular, it is recommended that they are not left openly on display in a vehicle or even at home!

1. I will not allow any other student to use the laptop at any time.
2. The Rooks Heath site insurance only covers the laptop whilst it is on the College's premises. It does not cover it in your home, at another site or whilst being transported to and from Rooks Heath.
3. Students granted the use of College's laptops are now held personally accountable for their damage at all times, and their loss or theft when away from the Rooks Heath College site, and will be expected to fully reimburse the College with the cost of a repair or replacement should their laptop be damaged, lost or stolen.
4. I understand that laptop computers are extremely vulnerable to theft and special care will be taken to avoid leaving my laptop in public view, either in a vehicle or even at home.
5. When the laptop cannot be with me, e.g. during PE lessons, it will be left safely with a member of staff.

By signing this form I confirm that I have read and agree to abide by these acceptable use rules and special conditions for use of a Rooks Heath College laptop computer.

Students Full Name:_____ ***Date:_____***

Students Signature:_____ ***Tutor Group:_____***

Parent/Carer Permission.
As the parent/carer of the student signing above, I agree to the terms and conditions above and grant permission for the student to have the use of a College's laptop computer during their time at Rooks Heath College. I understand that students will be held accountable for their own actions.

Parent/Carer Signature:_____ ***Date:_____***

Appendix C – E-Safe Incident log form

The College will keep an incident log and monitor the measures put in place. This will enable the College to know that the students are e-safe.

DATE: …….. **TIME:** ……..

INCIDENT LOGGED BY: ……

STUDENT(S) INVOLVED: ……

DETAILS OF THE INCIDENT: ……
…….
…….
…….
…….
…….
…….
…….
…….
…….

DATE WHEN PARENTS WERE CONTACTED (if a student): ……

ACTIONS TAKEN: ……
…….
…….
…….
…….
…….
…….

ADDITIONAL COMMENTS: ……
…….
…….
…….

Entered into E-Behaviour by: ……..

Signed: ……. Date: ……...

Appendix D

Acceptable use of Digital and ICT devices – Staff contract

The computer network, college funded laptops and mobile phones are owned by the College and are made available to staff to enhance their professional activities including teaching, research, administration, communication and management. The College reserves the right to examine or delete any files that may be held on its computer network, laptops or mobile phones to monitor any Internet sites visited by staff.

Members of Staff should regard the following guidelines for 'Acceptable use of Digital and ICT systems' as part of the College Staff Handbook and are required to comply with the guidelines.

1) All Internet activity should be appropriate to staff professional activity or students' education; If staff discover any unsuitable sites, the URL (website address) and content must be reported to the network manager who will arrange for its exclusion from future access;
2) Access to the network should only be made via the authorised username and password, which should not be made available to any other person;
3) Activity that threatens the integrity of the college ICT systems, or activity that attacks or corrupts other systems, is forbidden;
4) Members of Staff are responsible for email sent and contacts made that may result in email being received;
5) Use for personal financial gain, gambling, political purposes or advertising is forbidden;
6) Copyright of materials must be respected and sources acknowledged when used;
7) Posting anonymous messages and forwarding chain letters is forbidden;
8) As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
9) Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden;
10) Staff should not run social network spaces for students on a personal basis.
11) Staff should not give out their mobile number or home phone number to students. Staff should not use their personal phone or camera without permission e.g. for a college field trip. If personal equipment is being used it should be registered with the College and a clear undertaking that photographs will be transferred to the College network/MLE and will not be stored at home or on memory sticks and used for any other purpose than college approved business.
12) College laptops must not be left in an un-locked room.
13) Staff with responsibility for managing and accessing personal data in the College's Management Information System (Capita SIMS), the MLE (Canvas) or online reporting (MCAS), will comply with the following conditions:
    a. The data is to be used only for educational purposes.
    b. Personal data is to be shared only with those who need the information to discharge a statutory education function.
    c. Only authorised users may access the system and they must never share their login details with anyone.
    d. Management of Canvas usernames and passwords is the responsibility of the authorised system manager/MLE administrator in the college.
    e. Care will be taken to protect any data which is printed or otherwise displayed.
    f. Temporary data sets will be deleted as soon as possible.

Signed: …….. Date: …….

Name (Block Capitals): ……

Appendix E

Acceptable use of Mobile Phones issued by the College

The following requirements relate to mobile phones and are in addition to those listed and agreed in the ICT Acceptable Use Policy.

Mobile devices are configured to standard builds and tariff bands before delivery to the user. The College will monitor individual usage through itemised billing.

Issued mobile phones are for College business use. Usage should be reasonable and justified in relation to work. It is accepted that on some occasions personal usage may be necessary. This should be reasonable, not excessive and arrangements should be made to repay the costs of personal use if these exceed the monthly tariff.

It is the responsibility of the Head of Finance to check itemised bills, ensuring that call volumes and costs are appropriate and not excessive (for work purposes as well as any personal use). Where a user cannot justify call usage and costs on a repeated basis, it is the discretion of the Head Teacher, Director of Business or Associate Head Teacher to initiate disciplinary action in line with the Staff Disciplinary Policy.

Calls between the College mobiles are free. In order to help achieve best value for the College, staff issued with a mobile phone are expected to call these numbers from their mobile phone and not from a College landline. Therefore, these numbers should not be distributed to staff. Contact should be made via Reception in the usual manner.

College property

College purchased and leased mobile devices are College property (regardless of the source of funding). They are not a user's personal property nor are they available for individual resale or remuneration. All College purchased and issued mobile devices must be returned to the College upon termination of employment or on request. The College will securely erase data on mobile devices and reformat the device before re-issue to another college user. The device will also be securely erased when disposed of at the end of its lifecycle.

Reporting loss or theft of device

In the event of loss or theft of a mobile device the user should immediately report any theft to the Police and then inform the Assistant Business Manager. In relation to theft or loss of a mobile phone the user should also notify the Mobile provider directly on Tel: 0800 977 7337 or at http://service.o2.co.uk/IQ/srvs/cgi-bin/webcgi.exe?New,KB=Companion,T=contact_Us_Business

Signed: ……..... Date: …….

Name (Block Capitals): ……