Cranbury College IT Policy

The first two pages provide an easy-to-follow guide on the most important points of the Cranbury College IT Policy with the full version following on.

Summary

1. Cranbury College provide computers and the internet for work purposes, however a reasonable amount of personal use is ok as long as it doesn't get in the way of your own or anyone else's work and (for longer periods) you have checked that there is no-one that needs help. See 2.7.

2. Use common sense with internal/external emails& instant messages. Anything that is likely to cause offence, causes interruption to work or overloads the system is inappropriate. See 3.3.2.

3. Think about what you say electronically and how you say it be it email or anything else. Assume that anything you write may be accidentally sent to the wrong person or have to be disclosed, for example as part of legal proceedings against a decision we have made and word it on that basis. See 2.4.

4. You are privy to confidential information and have an obligation to keep it that way. That includes keeping your passwords secure and secret, and being careful how you store and send information. Sending information to a hotmail account for example may not be secure. See in particular 4.4 and 8.3 amongst others.

5. Illegal downloading or storage of illegal or illicit material on college computers is not allowed. If you are unsure as to whether what you are downloading/streaming is in breach of any copyright restrictions, then you shouldn't be doing it. See 7.1.9.

6. You can save music in your music folder but it must be legal and by saving it there you are taking responsibility for it being legally procured. Keep any other personal material stored on the network to a minimum and bear in mind that the college may ask you to remove it if it takes up too much space. If your music is saved on your hard drive note point (11) below and be prepared to lose it. See 6.5 and6.6.

7. Be aware that things you may think are deleted actually still exist on backups and in some circumstances may have to be disclosed. See 3.3.3 - 3.3.4.

8. If you use a college internet connection our IP address will be logged. Anything you post or otherwise upload or download can be traced to Cranbury College and we can trace it to you. Don't do anything that breaks the law or has the potential to embarrass Cranbury College. See 6.1.

9. In some exceptional circumstances you can be summarily dismissed for misuse of college equipment. Examples of this would be using any of the above means of communication for obscene, defamatory material or harassment. See 7.1.

10. Don't do anything that risks compromising our computer systems, think carefully about what you connect to USB ports, the emails that you open and the links that you click on. If you think that you may have done so then report to a member of the IT team or Chief Technology Officer immediately. The longer you leave it the more of a problem it will cause. See 8.9.

11. Don’t save anything important on your hard drive. It doesn’t get backed up and if your PC develops a fault you may lose it. See 6.6 and 8.10 - 8.12.

12. It’s your responsibility to look after any Cranbury College issued hardware that you take off site (eg laptops). Notify the police and college as soon as possible if it gets lost or stolen. See 2.8.

13. We may monitor your communications, but we’ll only do so if we have cause for concern. We won’t monitor communications as a matter of course. See 10.2.

14. Beyond college policies, there are criminal offences you should be aware of such as hacking and unauthorised modification of computer material. See 6.12.

15. Similarly the Data Protection Act means you and we have obligations to ensure personal data is kept secure. See 11.

16. Watching programmes streamed/downloaded from the internet is allowed but only from Youtube and UK hosted catch-up services linked to broadcasters such as BBC iPlayer, Sky Player, My5 etc. Watching anything streamed/downloaded from the internet that infringes copyright is not allowed. See 2.7.4.

17. If sending emails containing information or attachments of a confidential nature you should password protect these. See 3.2.5 and 3.2.6

Cranbury College IT Policy - September 2016

1. Introduction

1.1 All use of Cranbury College's communications facilities is governed by the terms of this policy. Any breach of this policy may lead to disciplinary action being taken against you and serious breaches may lead to summary dismissal. Please read this policy carefully.

1.2 Cranbury College's electronic communications systems and equipment are intended to promote effective communication and working practices within the organisation, and are critical to the success of our business. This policy outlines the standards Cranbury College requires users of these systems to observe, the circumstances in which Cranbury College will monitor use of these systems and the action we will take in respect of breaches of these standards.

1.3 Cranbury College's communications facilities are made available to users for the purposes of our business. A certain amount of limited and responsible personal use by users is also permitted. Note that some elements of personal use of Cranbury College's communications facilities are specifically addressed throughout this policy and particular attention should be paid to items 2.7, 3.3, 5, 8.12, 9.2, 10 and 11.

1.4 At Cranbury College, communication plays an essential role in the conduct of our business. How you communicate with people not only reflects on you as an individual but also on us as an organisation. We value your ability to communicate with colleagues, clients and business contacts, and we invest substantially in information technology and communications systems which enable you to work more efficiently. We trust you to use them responsibly.

1.5 This policy applies to all individuals working for Cranbury College at all levels and grades, who use our communications facilities, whether management committee, senior leaders, departmental heads, middle leaders, consultants, full-time, part-time or fixed-term employees, student teachers, trainees, contract staff, temporary staff, agency or home workers.

1.6 Although the detailed discussion is limited to use of email and internet facilities, the general principles underlying all parts of this policy also apply to telephone communications.

2. General Principles

2.1 You must use Cranbury College's information technology and communications facilities sensibly, professionally, lawfully, and consistently with your duties, with respect for your colleagues and for Cranbury College and in accordance with this policy and Cranbury College's other rules and procedures.

2.2 All information relating to our clients and our business operations is confidential. You must treat our paper-based and electronic information with utmost care.

2.3 Many aspects of communication are protected by intellectual property rights which are infringed by copying. Downloading, uploading, posting, copying, possessing, processing and distributing material from the internet may be an infringement of copyright or of other intellectual property rights.

2.4 Particular care must be taken when using Office 365, email, instant messaging, or internal message boards as a means of communication because all expressions of fact, intention and opinion in an email may bind you and/or Cranbury College and can be produced in court in the same way as other kinds of written statements.

2.5 The advantage of the internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. Internal comment and external feedback written on Office 365 or messages sent by email should be written as professionally as a letter or fax. Bear in mind we may have to disclose these externally, for example as part of legal proceedings against a decision we have made. You must not use these media to do or say anything which would be subject to disciplinary or legal action in any other context such as sending any discriminatory (on the grounds of a person's sex, race, disability, age, sexual orientation, religion or belief), defamatory, or other unlawful material (for example, any material that is designed to be, or could be construed as, bullying or harassment by the recipient). If you are in doubt about a course of action, take advice from your supervising line manager. You should assume that internal comments, external feedback written on Office 365 or messages sent by email may be read by others and not include in them anything which would offend or embarrass any reader, or you, if it found its way into the public domain.

2.6 Under no circumstances may Cranbury College's facilities be used in connection with the operation or management of any business other than that of Cranbury College or a client of Cranbury College unless express permission has been obtained from Cranbury College SLT.

2.7 Our overarching policy on personal usage of college IT resources (computers, internet connections etc.) is that this is a privilege and not a right.

2.7.1 Cranbury College permits you to use IT resources to a limited degree for personal use (eg internet banking, online shopping, facebook access, tv or music streaming) within working hours but this must not be at the expense of college business.

2.7.2 As a general rule short breaks in the working day where this activity takes place are permissible, but in the event of longer quiet periods of work you should check with your line manager and colleagues if there is other college related work that you can take on rather than using the internet for personal use.

2.7.3 If these activities require additional software to be installed onto your PC then you should submit a request via our IT support provider, Prospect School. Please liaise with the college IT Lead.Whenever you need to download additional software, you must obtain the express permission of the IT Lead who will consider the request in line with Cranbury College's policy.

2.7.4 Cranbury College allows you to watch streamed/downloaded programme or film content from some websites. We need to protect the college from copyright infringement and therefore we only allow access to a limited number of sites that provide legitimate access to this content. These sites are Youtube and legitimate UK hosted catch-up services linked to or licensed by broadcasters, such as iPlayer, ITV Player, 4oD, Sky Player, and My5. You may access these sites, for example at lunchtime or as part of your planning time if it is part of our lesson planning., as long as doing so does not interfere with your ability to perform your duties or detrimentally affecting the speed or reliability of the network. We have an automated system in place which blocks access to certain sites that are categorised as causing harm or offence, gambling, pornography and a few other categories. However this doesn't not ensure 100% compliance with this policy and it is your responsibility to ensure that you comply; if at any time you suspect what you are watching is in breach of the media owner's copyright, you must cease viewing this content.Cranbury College may, during periods it deems necessary through high demand, failure or any other reason ask you to refrain from using Audio and/or Video Streaming services so as to preserve bandwidth for business activities.

2.8 You have an obligation to look after IT equipment provided by Cranbury College and particular care should be taken over laptops and other portable equipment.

2.8.1 You should take good care of any laptop, tablet, mobile phone or other device given to you by the college and take all reasonable precautions to ensure that it is not damaged, lost or stolen.

2.8.2 In the event that a college device is lost or stolen, you will be expected to notify Cranbury College's Chief Technology Officer or the IT Support Team as soon as possible either in person or by phone. Due to the importance of data security and actions that need to be carried out reporting via email or text is not possible as this may cause a delay in the incident being acted upon.

2.8.3 In the event that a college device in your care is stolen, you willalso be expected to report the theft to the police and obtain a crime reference number. This number should also be given to Cranbury College; we may need this for insurance reasons.

2.8.4 Negligence in the care of college devices or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the staff member concerned. In these circumstances Cranbury College may prevent you from having future access to college devices.

2.8.5 Whilst particular risks apply to mobile devices, care should be taken when using any IT equipment provided by Cranbury College, including telephones on desks. These are expensive items and thus should be treated accordingly.

3. Use of Electronic Mail

3.1 Generally

3.1.1 Do not amend any messages received and, except where specifically authorised by the other person, do not access any other person's in-box or other email folders nor send any email purporting to come from another person, unless authorised to do so.

3.1.2 It is good practice to re-read and check an email before sending. Think about having someone second read any emails you have drafted that may be particularly contentious or delay sending it and reread it later.

3.1.3 If you copy an email to others, it may breach the Data Protection Act if it reveals all the recipients' email addresses to each recipient (e.g. in the case of marketing and mailing lists) and it can also breach duties of confidentiality (e.g. in the case of internal emails to members of a staff benefit scheme). Accordingly, it may be appropriate to use the 'Bcc' (blind carbon copy) field instead of the 'Cc' (carbon copy) field when addressing an email to more than one recipient. In general, it is not appropriate to Bcc people in other circumstances. If in doubt, seek advice from your line manager.

3.1.4 Cranbury College email is hosted by a third party. Whilst this means that our email is highly available from any connection to the internet, it also means that we must be extra vigilant with security and in particular ensuring secure passwords and not setting browsers on shared or public computers to store your email password.

3.1.5 Cranbury College do allow mobile devices both business and personal, by prior approval, to receive your work email. However, by doing so you grant Cranbury College permission to impose its security requirements on you and your device including device passcodes and auto-lock times.

3.2 Business Use

3.2.1 If the email message or attachment contains information which is time-critical, bear in mind that an email is not necessarily an instant or 100% reliable communication and consider whether it is the most appropriate means of communication.

3.2.2 If you have sent an important document, always telephone to confirm that the email has been received and read.

3.2.3 In light of the security risks inherent in some web-based email accounts such as Yahoo or Hotmail, you must not email business documents to your personal web-based accounts. You may send documents to a client's web-based account if you have the client's express written permission to do so. Only in exceptional circumstances should you send sensitive or highly confidential documents to a parents personal web-based email account, even if the parent asks you to do so.

3.2.4 Whilst our email service offers each user a generous amount of storage, this is limited. The bigger your mailbox the longer it will take to synchronise if your computer is swapped for another. It is therefore recommended to keep only attachments that are important. If you need to keep a large attachment for future reference, you should save this to your Office 365 Personal Drive.

3.2.5 If the email you are sending contains information of a highly confidential nature, then all confidential information should be stored in a password protected word document or zip file that is then attached to the email rather than the information being contained in the body the email. The password of the file should preferably be given in person or over the phone. If this is not practical the password should be sent in a separate email.

3.2.6 If you are sending an email with confidential attachments, these should first be zipped with a password and attached to the email. The password of the file should preferably be given in person or over the phone. If this is not practical the password should be sent in a separate email.

3.3 Personal Use

3.3.1 Although Cranbury College's email facilities are provided for the purposes of our business, we accept that you may occasionally want to use them for your own

personal purposes. This is permitted on the condition that all the procedures and rules set out in this policy are complied with. Be aware, however, that if you choose to make use of our facilities for personal correspondence, you can expect very little privacy because Cranbury College may need to monitor communications for the reasons given in item 10.2.

You must ensure that your personal email use:

(a) does not interfere with the performance of your duties;

(b) does not take priority over your work responsibilities;

(c) is minimal and limited to taking place substantially outside of normal working hours (i.e. during any breaks which you are entitled to or before or after your normal hours of work);

(d) does not cause unwarranted expense or liability to be incurred by Cranbury College;

(e) does not have a negative impact on Cranbury College in any way; and

(f) is lawful and complies with this policy.

3.3.2 You should not:

(a) send or forward private emails at work which you would not want a third party to read

(b) send or forward chain mail, junk mail or anything that breaches the college Dignity and Respect policy either within or outside Cranbury College;

(c) send trivial messages (cartoons, jokes, youtube links to the "*All Users" distribution list.

(d) contribute to system congestion by sending unwarranted high resolution images / movies or unnecessarily copying or forwarding emails to those who do not have a need to receive them; and

(e) download, store or email text, music, software, movie and other content on the internet subject to copyright protection unless it is clear that the owner of such works allows this.

3.3.3 You must not say anything in an email that would detrimentally affect the reputation of Cranbury College. As it is easy for emails to reach unintended recipients this policy applies to emails that are sent within Cranbury College as well as externally. You should also be aware that in some circumstances Cranbury College may be obliged to disclose emails that you have sent.

3.3.4 As with any correspondence made using Cranbury College's electronic facilities, you can delete personal emails from the live system, but they will reside in our email archive.

3.3.5 By making personal use of our facilities for sending and receiving email you signify your agreement to abide by the conditions imposed for their use, and signify your consent to Cranbury College monitoring your personal email in accordance with section 10 of this policy.

4. USE OF OFFICE 365

4.1 **PARTICULAR CARE SHOULD BE TAKEN TO ENSURE THE CONFIDENTIALITY OF INFORMATION RECEIVED ON OFFICE 365. NO INFORMATION RECEIVED BY CRANBURY COLLEGE ON OFFICE 365 SHOULD BE DISCUSSED OUTSIDE CRANBURY COLLEGE OTHER THAN SPECIFICALLY WITH THE PERSON THAT SENT THE INFORMATION UNLESS THERE IS A CLEAR BUSINESS JUSTIFICATION FOR DOING SO, E.G. RESPONDING TO A COMPLAINT. IF IN DOUBT, CHECK WITH YOUR LINE MANAGER.**

4.2 **CARE MUST ALWAYS BE TAKEN WITH THE CLARITY AND TONE OF EXTERNAL FEEDBACK WRITTEN ON OFFICE 365 AS THESE MAY LATER BE SUBJECT TO SCRUTINY IN THE EVENT OF LEGAL PROCEEDINGS.**

4.3 **CARE MUST ALSO BE TAKEN WITH THE TONE OF INTERNAL COMMENTS WRITTEN ON OFFICE 365 AS THESE MAY ALSO BE LATER SUBJECT TO SCRUTINY IN THE EVENT OF LEGAL PROCEEDINGS.**

4.4 **BREACH OF CONFIDENTIALITY, OR USE OF OFFICE 365 IN ANY OTHER WAY THAT WILL DETRIMENTALLY AFFECT THE REPUTATION OF CRANBURY COLLEGE**will be treated seriously and dealt with in accordance with Cranbury College's disciplinary procedure. In some circumstances this could also lead to summary dismissal.

5. Personal Blogs, Websites, Social Networking Sites and Twitter.

5.1 Cranbury College recognise that in your own private time you may wish to publish content on the internet. **This part of the policy and procedures in it apply to content that you publish on the internet (e.g. your contributions to blogs, message boards and social networking or content-sharing sites) even if created, updated, modified or contributed to outside of working hours or when using personal IT systems.**

5.2 If you post any content to the internet, written, vocal or visual, which identifies, or could identify, you as a member of Cranbury College staff and/or you discuss your work or anything related to Cranbury College or its business, customers or staff, Cranbury College expects you, at all times, to conduct yourself appropriately and in a manner which is consistent with your contract of employment and with Cranbury College's policies and procedures. It should be noted that simply revealing your name or a visual image of yourself could be sufficient to identify you as an individual who works for Cranbury College.

5.3 If you already have a personal blog or website which indicates in any way that you work for Cranbury College you should report this to your line manager.

5.4 If you intend to create a personal blog or website that will say that you work for Cranbury College, or in any way could identify you as someone who works for Cranbury College then you should report this to your line manager.

5.5 If a blog posting clearly identifies that you work for Cranbury College and you express any idea or opinion then you should add a disclaimer such as "these are my own personal views and not those of Cranbury College".

5.6 Care should be taken when accessing or updating a personal blog or website from Cranbury College's computers or during work time as some sites and systems record date, time and source location of changes. If you are likely to be in a position where a client has reason to complain you haven't had a chance to do something for them but have been able to update

your personal blog or website then you are likely to be in breach of the reasonable personal use of the internet provided for by this policy.

5.7 The following matters will be treated as gross misconduct capable of resulting in summary dismissal (this list is not exhaustive):

5.7.1 Revealing confidential information about Cranbury College in a personal online posting. This might include revealing information relating to Cranbury College's clients, business plans, policies, staff, financial information or internal discussions. Consult your manager if you are unclear about what might be confidential.

5.7.2 Criticising or embarrassing Cranbury College, its clients, its stakeholders or its staff in a public forum (including any website). You should respect the reputation of Cranbury College and the privacy and feelings of others at all times. If you have a genuine complaint to make about a colleague or workplace matter the correct procedure is to raise a grievance using Cranbury College's grievance procedure.

5.7.3 Excessively accessing or updating personal blogs, websites or social networking sites from Cranbury College's computers or during work time.

5.8 If you think that something on a blog or a website could give rise to a conflict of interest and in particular concerns issues of impartiality or confidentiality required by your role then this must be discussed with your line manager.

5.9 If someone from the media or press contacts you about your online publications that relate to Cranbury College you should talk to a member of the Cranbury College Senior Leadership Team.

5.10 Online publications which do not identify the author as a member of Cranbury College staff and do not mention Cranbury College and are purely concerned with personal matters will normally fall outside the scope of Cranbury College's communications policy.

6. Use of Computers, Internet and Network

6.1 We trust you to use the internet sensibly. Bear in mind at all times that, when visiting a website, information identifying your PC and Cranbury College may be logged by that site. Therefore any activity you engage in via the internet may affect Cranbury College and can be easily traced back to Cranbury College. For example, changes made to a page on Wikipedia or comments made anonymously on a forum could be traced back to Cranbury College.

6.2 Cranbury College servers keep a log of every webpage you visit (for a period of less than a year) from within Cranbury College's network for compliance purposes. Whilst we won't routinely look at an individual's activity we reserve the right to should we have reason to believe that any part of this policy concerned with network/internet use has been breached.

6.3 Whenever you access a web site, you should always comply with:

- The terms and conditions governing its use.
- This policy
- UK law

6.4 Cranbury College provide a standard image for desktop PCs and laptops which includes all software that an individual will need to carry out their duties. No additional software should be installed without the express permission of the IT Lead. Requests for installation of additional software must be provided in writing to the IT Lead and will be considered but will require the software in question to be tested before it can be approved to check that it will in

no way adversely affect the operation of any part of Cranbury College's IT infrastructure. This includes the purchase of software and Software as a Service(SaaS)/Cloud services.

6.5 You can save music in your music folder but it must be legal and by saving it there you are taking responsibility for it being legally procured and that you are complying with Copyright law.

6.6 You must not save anything important on your hard drive as it does not get backed up. Should your hard drive fail, Cranbury College will not endeavour to recover material stored on it. Cranbury College reserves the right to wipe anything on your computer's hard disk at any time without warning.

6.7 You are strongly discouraged from providing your Cranbury College email address when using public websites for non-business purposes, such as online shopping. This must be kept to a minimum and done only where necessary, as it results in you and Cranbury College receiving substantial amounts of unwanted email.

6.8 You must not post your Cranbury College email address on any message boards, blogs or other generally accessible web pages unless there is a business justification. If you are in doubt about this then check with your line manager.

6.9 Cranbury Collegesystems automatically block access to some websites that are categorised as containing material that could have a detrimental effect on one or more members of staff's ability to perform their duties or on any part of Cranbury College's IT Infrastructure. Cranbury College reserve the right to block access to any website it sees necessary to protect its staff, reputation and data security.

6.10 Cranbury College's IT infrastructure must not be used for any activity involved in gaining access to any remote system for which you have not been granted access to by the owner.

6.11 You must not:

6.11.1 introduce packet-sniffing, password-detecting, keylogging or remote monitoring software;

6.11.2 seek to gain access to restricted areas of Cranbury College's network;

6.11.3 access or try to access data which you know or ought to know is confidential;

6.11.4 intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software; nor

6.11.5 carry out any hacking activities

6.11.6 visit websites you know or suspect may contain material:

- in breach of UK copyright or any other law
- Infected with or containing a virus, spyware or malware

6.12 For your information, breach of any of the provisions of items 6.11.1 to 6.11.6 (inclusive) above would not only contravene the terms of this policy but could in some circumstances also amount to the commission of an offence under the Computer Misuse Act 1990, which creates the following offences:

6.12.1 unauthorised access to computer material ie hacking;

6.12.2 unauthorised modification of computer material; and

6.12.3 unauthorised access with intent to commit or facilitate the commission of further offences.

7. Misuse of Cranbury College's Facilities and Systems

7.1 Misuse of Cranbury College's facilities and systems, including its telephone, email and internet systems, in breach of this policy will be treated seriously and dealt with in accordance with Cranbury College's disciplinary procedure. In particular, viewing, accessing, transmitting, posting, reproducing, downloading or uploading any of the following materials in the following ways, or using any of Cranbury College's facilities, will amount to gross misconduct capable of resulting in summary dismissal (this list is not exhaustive), except where it can be clearly demonstrated that it is directly related to Cranbury College business:

7.1.1 material which is sexist, racist, homophobic, xenophobic, pornographic, paedophilic or similarly discriminatory and/or offensive;

7.1.2 offensive, obscene, derogatory or criminal material or material which is liable to cause embarrassment to Cranbury College and any of its staff or its clients or bring the reputation of Cranbury College and any of its staff or its clients into disrepute;

7.1.3 any defamatory material about any person or organisation or material which includes statements which are untrue or of a deceptive nature;

7.1.4 any material which, by intent or otherwise, harasses the recipient;

7.1.5 any other statement which is designed to cause annoyance, inconvenience or anxiety to anyone;

7.1.6 any material which violates the privacy of others or unfairly criticises or misrepresents others;

7.1.7 confidential information about Cranbury College and any of its staff or clients;

7.1.8 any other statement which is likely to create any liability (whether criminal or civil, and whether for you or Cranbury College);

7.1.9 material in breach of copyright and/or other intellectual property rights;

7.1.10 online gambling; or

7.1.11 unsolicited commercial or advertising material, chain letters or other junk mail of any kind.

7.2 If Cranbury College has evidence of the examples of misuse set out in 7.1.1 to 7.1.11 above it reserves the right to undertake a more detailed investigation in accordance with its disciplinary procedures.

8. System Security

8.1 Security of our IT systems is of paramount importance. We are both contractually obliged and owe a duty to all of our clients to ensure that all of our business transactions are kept confidential. If at any time we need to rely in court on any information which has been stored

or processed using our IT systems it is essential that we are able to demonstrate the integrity of those systems. Every time you use the system you take responsibility for the security implications of what you are doing.

8.2 Cranbury College's systems or equipment must not be used in any way which may cause damage, or overloading or which may affect its performance or that of the internal or external network.

8.3 Keep all confidential information secure, use it only for the purposes intended and do not disclose it to any unauthorised third party. Failure to do so will be treated seriously and dealt with in accordance with Cranbury College's disciplinary procedure.

8.4 Keep your system passwords safe. Do not disclose them to anyone or record them. Those who have a legitimate reason to access other users' inboxes will be given access through their own login credentials by IT support. If it is discovered that you have disclosed your password to anyone else, which you must not do, you will be forced to change your password when you next login. You will not be able to use the same password.

8.5 When setting a password you must ensure that you have taken reasonable precautions to ensure that it will not be guessed. Additionally your passwords:

8.5.1 Must be at least 8 characters in length (although the longer the better)

8.5.2 Must not be identical to or very close to a password for another system be it for work or for personal. Eg GiraffeDog2012 and GiraffeDog2013.

8.5.3 Must contain characters from at least three of the following categories:

(a) English uppercase characters (A through Z)

(b) English lowercase characters (a through z)

(c) Numbers (0 through 9)

(d) Non-alphanumeric characters (e.g. !, $, ^, %, &) *Note: some systems don't allow certain characters*

8.5.4 You should take care to ensure that your password doesn't include words that can easily be attributed to Cranbury College, yourself or your role. This includes using part or whole of your name, Cranbury College or associated names, your job role or associated activities or the name of any Cranbury College system or service e.g. Office 365, Adway.

8.6 If a document is highly commercially confidential or price sensitive, you should store it in a private area of the network. Every user has their own personal storage (H drive) on the network that only they can access. There are also other restricted storage areas on the network that are for storage of documents relating to particular areas of the business such as HR or Finance. Access to these locations is restricted to only those users who need access as part of their role at Cranbury College.

8.7 Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner. Cranbury College provide special bins for unwanted confidential documents and paperwork, the contents of which are safely and securely disposed of.

8.8 You should not download or install software from external sources without having first received the necessary authorisation from the Chief Technology Officer. This includes

software programs, instant messaging programs, screensavers, photos, video clips and music files.

8.9 Connection of external devices and equipment including but not limited to discs, USB flash drives, and other data storage devices, MP3 players or similar devices, PDAs and mobile phones to Cranbury College's systems is allowed but every care must be taken not to introduce any virus, spyware or other malicious programme purposely or by accident. This is a privilege and not a right. Cranbury College reserve the right to withdraw this privilege if it is deemed necessary.

8.10 At any time, and without notice Cranbury College may replace your desktop PC with an equivalent pc containing only the standard Cranbury College image, for example in the event of hardware failure. As a result storing of personal data on your desktop is not advisable and Cranbury College take no responsibility for loss of any personal data and will make no attempt to recover it.

8.11 You should always exercise caution when opening emails from unknown external sources or following links to pages on the internet, or where, for any reason, an email appears suspicious. Where you have cause to believe you may have exposed Cranbury College's IT infrastructure to risk you should notify the Chief Technology Officer or IT Teamimmediately.

8.12 Any data stored by you should always be stored on 'h' drives rather than 'c' drives in order to ensure data is not lost. Cranbury College believes you should have sufficient data storage in able to do your job and we do not cap storage per user, however in return we expect staff to think carefully about what you store and why you need to store it. Storage of personal data is a privilege and Cranbury College reserve the right to withdraw this at any time. For example, personal data may be deleted to keep the business operating in the event that network drives become unexpectedly or unnecessarily full.

9. Remote Connectivity

9.1 This part of the policy and the procedures in it apply to your use of our systems, to your use of our laptops, and also to your use of your own computer or electronic equipment including smartphones, PDAs and netbooks or other computer equipment (eg client's equipment) whenever you are working on Cranbury College's business away from Cranbury College's premises (working remotely) or using any such equipment that connects to Cranbury College's infrastructure.

When you are working remotely you must:

9.1.1 password protect any work which relates to Cranbury College's business so that no other person can access your work;

9.1.2 position yourself so that your work cannot be seen by any other person;

9.1.3 take reasonable precautions to safeguard the security of our equipment, and keep your passwords secret;

9.1.4 inform the police and our IT department (as appropriate) as soon as possible if either a Cranbury College laptop in your possession or any computer equipment on which you do Cranbury College's work or access Cranbury College's Data, even if this is personal IT equipment or mobile device, has been lost or stolen; and

9.1.5 ensure that any work which you do remotely is saved on Cranbury College's system or is transferred to our system as soon as reasonably practicable.

9.1.6 Use of web based email to send documents to Cranbury College should be avoided

9.2 Pocket computers, mobile phones and similar hand-held devices are easily lost or stolen so you must password-protect access to any such devices used by you on which is stored or can access any personal data of which Cranbury College is a data controller or any information relating our business, our clients or their business. You must inform Cranbury College as soon as possible if an electronic device which connects to Cranbury College's infrastructure is lost or stolen so that passwords can be changed to block access from these devices by unauthorised persons.

10. Monitoring of Communications by Cranbury College

10.1 Cranbury College is ultimately responsible for all communications using college resources but subject to that will, so far as possible and appropriate, respect your privacy and autonomy while working. Cranbury College's general practice on monitoring is that we will monitor communications where there is a cause for concern and we will not monitor individual communications as a matter of course.

10.2 Cranbury College may monitor your business communications for reasons which include:

10.2.1 providing evidence of business transactions;

10.2.2 ensuring that Cranbury College's business procedures, policies and contracts with staff are adhered to;

10.2.3 complying with any legal obligations;

10.2.4 monitoring standards of service, staff performance, and for staff training;

10.2.5 preventing or detecting unauthorised use of Cranbury College's communications systems or criminal activities; and

10.2.6 maintaining the effective operation of Cranbury College's communications systems.

10.3 Cranbury College may monitor telephone, email and internet traffic data (ie sender, receiver, subject; non-business attachments to email, numbers called and duration of calls; domain names of websites visited, duration of visits, and files downloaded from the internet) at a network level (but covering both personal and business communications) for the purposes specified at item 10.2. For the purposes of your maintenance of your own personal privacy, you need to be aware that such monitoring might reveal sensitive personal data about you. For example, if you regularly visit websites which detail the activities of a particular political party or religious group, then those visits might indicate your political opinions or religious beliefs. By carrying out such activities using Cranbury College's facilities you consent to our processing any sensitive personal data about you which may be revealed by such monitoring.

10.4 Sometimes it is necessary for Cranbury College to access your business communications during your absence, such as when you are away because you are ill or while you are on holiday. Unless your mailbox settings are such that the individuals who need to do this already have permission to view your inbox, access will be granted only with the permission of one of the persons authorised to grant such access.

10.5 If external parties inform you that emails they have sent to any address at Cranbury College have been bounced back you must inform IT Support at the earliest opportunity.

11. Data Protection

11.1 As a member of Cranbury College who uses our communications facilities, you will inevitably be involved in processing personal data for Cranbury College as part of your job. Data protection is about the privacy of individuals, and is governed by the Data Protection Act 1998. This Act defines, among others, terms as follows:

11.1.1 "data" generally means information which is computerised or in a structured hard copy form;

11.1.2 "personal data" is data which can identify someone, such as a name, a job title, a photograph;

11.1.3 "processing" is anything you do with data – just having data amounts to processing; and

11.1.4 "data controller" is the person who controls the purposes and manner of processing of personal data – this will be Cranbury College, in the case of personal data processed for the business.

11.2 Whenever and wherever you are processing personal data for Cranbury College you must keep it secret, confidential and secure, and you must take particular care not to disclose them to any other person (whether inside or outside Cranbury College) unless authorised to do so. Do not use any such personal data except as authorised by Cranbury College for the purposes of your job. If in doubt get help from our Data Protection Officer or your line manager.

11.3 The Data Protection Act gives every individual the right to see all the information which any data controller holds about them. Bear this in mind when recording personal opinions about someone, whether in an email or otherwise. It is another reason why personal remarks and opinions must be made or given responsibly, and they must be relevant and appropriate as well as accurate and justifiable.

11.4 For your information, section 55 of the Data Protection Act provides that it is a criminal offence to obtain or disclose personal data without the consent of the data controller. "Obtaining" here includes the gathering of personal data by employees at work without the authorisation of the employer. You may be committing this offence if without authority of Cranbury College: you exceed your authority in collecting personal data; you access personal data held by Cranbury College; to control it or you pass them on to someone else (whether inside or outside Cranbury College).

11.5 While Cranbury College is a data controller of all personal data processed for the purposes of our business, you will be a data controller of all personal data processed in any personal email which you send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the Data Protection Act, but if, in breach of this policy, you are using our communications facilities for the purpose of a business which is not Cranbury College's business, then you will take on extensive personal liability under the Data Protection Act.

11.6 To help you understand and comply with Cranbury College's obligations as a data controller under the Data Protection Actyou may be offered, and you may also request, training. Whenever you are unsure of what is required or you otherwise need guidance in data protection, you should consult our Data Protection Officer.

12. COMPLIANCE WITH THIS POLICY

12.1 Failure to comply with this policy may result in disciplinary action being taken against you under Cranbury College's disciplinary procedures, which may include summary dismissal, and/or in the withdrawal of permission to use the colleges equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager.

12.2 Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes [and updates will be published on our website].