Robert Carre Trust
ICT Acceptable Use Policy (Staff)

1 Introduction

1.1 ICT is provided to support and improve the teaching and learning in our Trust as well as ensuring the smooth operation of our administrative and financial systems.

1.2 This policy sets out our expectations in relation to the use of any computer or other electronic device on our network, including how ICT should be used and accessed within the Trust.

1.3 The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time, however a breach of this policy is likely to result in disciplinary action.

2 Scope and Purpose

2.1 This policy applies to all employees, governors, volunteers, visitors and any contractors using our ICT facilities. Ensuring ICT is used correctly and properly and that inappropriate use is avoided is the responsibility of every employee. If you are unsure about any matter or issue relating to this policy you should speak to the ICT Services Manager / Network Manager or Executive Headteacher / Head of School.

2.2 The purpose of this policy is to ensure that all employees are clear on the rules and their obligations when using ICT to protect the Trust and its employees from risk.

2.3 Employees may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

2.4 Any failure to comply with this policy may be managed through the disciplinary procedure. A serious breach of this policy may be considered as gross misconduct which could lead to dismissal.

2.5 If you reasonably believe that a colleague has breached this policy you should report it without delay to the ICT Services Manager / Network Manager or Executive Headteacher / Head of School.

3 Monitoring

3.1 The contents of our ICT resources and communications systems held in whatever media, including information and data held on computer systems, hand-held devices, tablets or other portable or electronic devices and telephones, relating both to the Employer's own education provision or any pupils, clients, suppliers and other third parties with whom the Employer engages or provides educational provision for, remains our property. Therefore, employees should have no expectation of privacy in any message, files, data, document, facsimile, social media post, blog, conversation or message, or any other kind of information or communication transmitted to, received or printed from, or stored or recorded on our electronic information and

communications systems. Do not use our ICT resources and communications systems for any matter that you wish to be kept private or confidential.

3.2 We may monitor, intercept and review, without notice, employee activities using our ICT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and are for legitimate business purposes. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

3.3 We will comply with the requirements of Data Protection Legislation (being (i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998) in the monitoring of our IT resources and communication systems and monitoring undertaken is in line with our Workforce Privacy Notice which sets out how we will gather, process and hold personal data of individuals during their employment. Our Data Protection Policy sets out how we will comply with Data Protection Legislation.

3.4 In line with the requirements of Data Protection Legislation, we may store copies of data or communications accessed as part of monitoring for a period of time after they are created, and may delete such copies from time to time without notice. Records will be kept in accordance with our **Records Management Policy**.

4 The Trust Image

4.1 Trust ICT facilities shall not be used in any way that could be damaging to the Robert Carre Trust's public image, or for purposes not in the interest of the Trust, or is abusive, offensive, defamatory, obscene or indecent or of such a nature as to bring the Trust or its staff and pupils into disrepute.

5 Internet Safety

5.1 Never give out personal information such as your address, telephone number or mobile number over the internet without being sure that the receiver is from a reputable source.

5.2 Never give out personal information about a pupil or another employee over the internet without being sure that the request is valid and you have the permission to do so.

5.3 Always alert the ICT Services Manager / Network Manager if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on our network will be subject to monitoring.

5.4 Always alert the ICT Services Manager / Network Manager if you receive any messages that make you feel uncomfortable or you think are unsuitable.

6 Internet and E-mail

6.1 The internet and email facilities are provided to support the aims an objective of the Trust. Both should be used with care and responsibility.

6.2 Use of the internet at work must not interfere with the efficient running of the Trust. We reserve the right to remove internet access to any employee at work.

6.3 You must only access those services you have been given permission to use.

6.4 Before sending an email, you should check it carefully and consider whether the content is appropriate. You should treat emails like you would any other form of formal written communication.

6.5 Although the email system is provided for business purposes we understand that employees may on occasion need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect, or be to the detriment of, you carrying out your role effectively. When sending personal emails from your work email account you should show the same care in terms of content as when sending work-related emails.

6.6 The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be considered under the disciplinary procedure.

6.7 You should not send electronic messages which are impolite, use obscene language, are indecent, abusive, discriminating, racist, homophobic or in any way intended to make the recipient feel uncomfortable. This will be considered under the disciplinary procedure.

6.8 If you receive an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, you should not forward it to any other address but you should alert the ICT Services Manager / Network Manager.

6.9 Do not access any sites which may contain inappropriate material or facilities, as described below:

i. Proxy
ii. Dating
iii. Hacking software
iv. Pornographic content
v. Malicious content
vi. Music downloads
vii. Non-educational games
viii. Gambling

6.10 Do not send malicious or inappropriate pictures of children or young people including pupils, or any pornographic images through any email facility. If you are involved in these activities the matter may be referred to the police.

6.11 Under no circumstances, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or young people. This material includes, but is not limited to pornography, unethical or illegal requests, racism, sexism, homophobia, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials you must inform the ICT Services Manager / Network Manager.

6.12 Do not upload or download unauthorised software and attempt to run on a networked computer; in particular hacking software, encryption and virus software.

6.13 Do not use the computer network to gain unauthorised access to any other computer network.

6.14 Do not attempt to spread viruses.

6.15 Do not transmit material subject to copyright or which is protected by trade secret which is forbidden by law.

6.16 Never open attachments of files if you are unsure of their origin; delete these files or report to the ICT Services Manager / Network Manager.

6.17 Do not download, use or upload any material from the internet, unless you have the owner's permission.

6.18 Do not send personal data via unencrypted e-mails.

6.19 If sending one e-mail to multiple external recipients ensure contact addresses are entered using the 'Bcc' field rather than the 'To' field so they are not visible to the other recipients.

6.20 Ensure sensitive or confidential data is not shared with others especially if projecting their screen within a classroom or hall.

7 Computer Equipment

7.1 The acquisition and utilisation of computer equipment and software requires the approval of the ICT Services Manager in order to ensure system compatibility and compliance with the ICT strategy endorsed by the Trustees of the Robert Carre Trust.

7.2 All computer equipment shall be kept in a secure location.

7.3 Only ICT Support and Site staff are permitted to move desktop computers and printers. Users must not move these items and should notify ICT Support if an item requires movement to a new location so that current Health and Safety requirements and network compatibility is met.

7.4 No personal computer hardware is to be connected to the Trust's network without prior permission of the ICT Services Manager.

7.5 It is the responsibility of the user of portable equipment to ensure its security at all times. This requires the user of portable equipment to ensure:

i. It is locked away and out of sight when not in use;
ii. It is secured whilst in use and left unattended temporarily (e.g. laptop security cable or similar);
iii. That equipment is not planned to be left unattended in a vehicle. If a user does have to leave the equipment unattended, it must be securely locked away in the boot of their car;
iv. Equipment must never be left visible in a vehicle, even when the vehicle is occupied.

7.6 Users are responsible for all portable equipment and accessories issued to them and are required to look after, transport and store the equipment effectively in order to prevent damage to the equipment and accessories.

7.7 Users are only permitted to use the portable equipment of the Trust that is issued to and signed for by them, and thereby authorised for their professional use.

7.8 Persons leaving the employment of the Trust must return all portable computer equipment and accessories before departure.

7.9 Users are required to be careful in their use of IT equipment, taking all reasonable steps to avoid damage to, or loss of, IT equipment and data. Levels of damage/loss will be monitored and reported to the Headteacher.

7.10 The disposal of computer equipment requires the approval of the ICT Services Manager in order to ensure asset replacement and disposal procedure compliance.

8 Computer System Security Access

8.1 Access levels to the computer systems, user identifications and password systems, will be set and managed by the ICT Services Manager in consultation with the Executive Headteacher.

8.2 Users must never disclose their user identities or passwords to any other person. They should ensure that their passwords are changed regularly and must not write down passwords under any circumstances (e.g. in diaries, post-it notes).

8.3 Users must ensure that they log out of the system after use and do not leave the computer unattended whilst it is still logged into the system. The computer can be left unattended and logged on for short periods of time, but in those circumstances the computer must be locked using the 'Lock this computer' or 'Lock' facility of Microsoft Windows.

8.4 Forgotten passwords will be reset only by a member of ICT Support.

8.5 Users must not log onto the network to facilitate colleagues/others using the network (see 9).

8.6 Users must not give individuals from outside the Trust access to the Trust's computer systems. This includes, but is not limited to, allowing family members or friends access to Trust computer equipment.

9 Computer System Security and Usage

9.1 Users will not download software programmes for use on the network without authorisation from the ICT Services Manager. Documents and files downloaded must be for business use only.

9.2 Any alteration to the data of other staff without their explicit authorisation is prohibited.

9.3 Attempting to hack into the network or enabling the malicious introduction of viruses, Trojans etc contravenes the Computer Misuse Act 1990.

9.4 Data stored on the local hard disk (e.g. C:\ or D:\ drive) of portable equipment cannot be backed up from the network and it is therefore the responsibility of the individual to make regular backups.

9.5 Any large or sustained transfers of data likely to interfere with the normal operation of the network are to be notified by users to ICT Support in advance of the transfer.

9.6 Deliberate unauthorised access to, copying, alteration, or interference with Trust computer applications or data is not allowed.

9.7 All computer applications and data developed for the Trust are for the sole use of the Trust except by permission of the Executive Headteacher.

9.8 Users should ensure they DO NOT use external storage devices (e.g. USB memory sticks) as a storage medium for their Trust data. External storage should only be used to transfer data from one location to another (e.g. home to Trust) where the use of the computer network and/or Internet is not possible (or practical). External storage devices are easily lost, stolen and the contents corrupted. As these devices do not connect to the Trust's computer network we are unable to recover any lost data. All Trust data should be saved to the Trust network (e.g. Home drive or shared drive) where it can be regularly backed up. Any data saved on the Trust system can be accessed at Trust sites and from home through the Trust's website(s). You must not use external storage devices where you are unsure of the content or origin.

NB: No data, including but not limited to information about students (e.g. class lists, registers and reports), should ever be saved to an unencrypted storage device as this contravenes the General Data Protection Regulations (GDPR).

9.9 Where business case laptop users choose to install applications, such as, but not limited to, iTunes and BBC iPlayer they must ensure media files are not saved on the Trust network (e.g. Home drive or shared drive).

9.10 System storage space is finite and users should routinely remove or archive old files from the Trust networked systems (e.g. Home drive and shared drives). Failure to do so may result in a user or users being unable to save their work, or in the worst case, account failure.

9.11 E-mail storage space is finite and users should routinely remove or archive messages from their Inbox (including any subfolders), Sent Items and Deleted Items. Failure to do so will result in the user being unable to send or receive e-mails.

10 Potential to cause Offence

10.1 Trust ICT facilities shall not be used for any activity that will cause offence to Robert Carre Trust staff, students, suppliers, partners or visitors.

11 Bring Your Own Device (BYOD)

11.1 Staff choosing to connect their personal devices to the Trust's wireless network accept that, where appropriate, they must comply with the requirements and terms of this policy.

11.2 Staff incorporating BYOD as part of an ICT enriched curriculum must be familiar with, and ensure students abide by, the Trust's **ICT Bring Your Own Device (BYOD) policy**

11.3 The Trust accepts no liability in respect of any loss/damage to personal ICT devices while at a Trust site or during Trust-sponsored activities. The decision to bring a personal ICT device onto a Trust site rests with the member of staff, as does the liability for any loss/damage that may result from the use of a personal ICT device on a Trust site.

11.4 Staff are responsible for charging their personal ICT devices prior to bringing them onto a Trust site. Personal ICT devices cannot be connected to Trust power outlets without first being PAT tested by one of the Trust's designated PAT testers.

12 Personal Use

12.1 Trust ICT facilities are there to support our Trust. The Executive Headteacher may choose to permit limited personal use as long as this does not conflict or interfere with normal Trust activities.

12.2 Any such personal use must comply with all the requirements and terms of this policy.

12.3 Personal use will only be authorised for the user, it shall not be extended to any other person. This includes, but is not restricted to, family members or friends.

12.4 The personal use of social networking websites such as, but not limited to, Facebook and Twitter is prohibited; this applies at all times including personal and home use.

NB: this does not apply to the use of these sites as a marketing or communication tool. In such cases staff must not use their own personal account(s), they will be provided with a Trust account that can be monitored and moderated by nominated groups or individuals as appropriate. The use of social networking as a marketing or communication tool is guided by the **Social Media Policy**.

12.5 The personal use of any site blocked by the Trust's Network is prohibited; this applies at all times including personal and home use.

12.6 Users are not permitted to save personal media to the Trust networked systems (e.g. Home drive or shared drives). This media includes, but is not limited to, audio, video and image files. Any such media will be removed by ICT Support in consultation with the user.

13 General

13.1 It is the responsibility of the ICT Services Manager to ensure adequate back-up procedures are in place at all times. Back up must be carried out on at least a daily basis.

13.2 The ICT Services Manager will ensure portable devices issued to staff (e.g. laptops and tablets) are encrypted. Staff are forbidden from removing, or attempting to remove, encryption from any portable device.

13.3 All staff are required to report violations of the security procedures established within this security policy direct to the ICT Services Manager who will work with Line Managers and the Executive Headteacher to resolve/address the problem.

13.4 The requirements contained in this policy statement are of a general nature covering all computers. Additionally there may be requirements designed for specific equipment and sites.

13.5 Rooms where computers are installed and stored must be adequately protected. Staff must ensure these rooms are locked when not supervised.

13.6 Keys for secure areas (rooms, safes, etc) must not be handed to unauthorised individuals.

13.7 Waste computer printed output must be disposed of with due regard to its sensitivity. Confidential output must be shredded and, if necessary, guidance should be sought from the Director of Finance, Administration and Resources or through the **GDPR policy**.

13.8 The use of ICT shall not disrupt the intended use of system or network resources and shall be appropriate for the task. Users shall avoid excessive, unnecessary consumption of computing resources for either personal or business use.

13.9 Home PCs used for work purposes must be managed effectively if they are used to transmit or store material connected to professional business. Confidential data, including any personal data on students, must not be stored on home PCs. General Trust data should be stored on the home PC for only as long as is absolutely necessary.

13.10 The use of computing resources is subject to UK law and any illegal use will be dealt with appropriately.

14 Prohibited Acts

The following acts are prohibited in relation to the use of Trust ICT systems and will not be tolerated:

14.1 Violating copyright laws

14.2 Attempting to harm minors in any way

14.3 Impersonation of any person or entity, or to falsely state or otherwise misrepresent an affiliation with a person or entity

14.4 Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service

14.5 Uploading, posting, messaging or otherwise transmitting any content that without the right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements)

14.6 Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party

14.7 Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.

14.8 "Stalking" or otherwise harassing any user or employee

14.9 Collection or storage of personal data about other users

15 Disciplinary Action

15.1 Any member of staff in breach of this policy may find themselves liable to disciplinary action. Disciplinary action will be automatically taken for unauthorised disclosure of Trust data or malicious damage.

16 Compensation

16.1 The Trust may seek to recover costs from a member of staff who is in breach of this policy in relation to the replacement of equipment or time spent re-securing the network.

Reviewed at the meeting of the Education and Personnel Committee on 25 June 2018

Ratified at the meeting of the Board on 12 September 2018

Next Review Due: September 2020 (2 years)