ICT User Policy

for use in

Essa Academy

Essa Primary Academy

Essa Nursery

and

Support Services

For approval and adoption by the Board of Directors- 7 July 2017

For adoption by Essa Academy LGB- 19 September 2017

For adoption by Essa Primary Academy LGB- 20 September 2017

For adoption by Essa Nursery Management Committee- Sept 2017

Written by- Paul Gartland

Date for Review- Spring 2020

Contents

1. Introduction

1.1 The Board of Directors is responsible for approving this policy and for ensuring it is implemented throughout the trust's senior leadership and support services. LGBs are responsible for adopting this policy and for ensuring its implementation in their academies. The Nursery Management Committee is responsible for adopting this policy and ensuring its implementation in Essa Nursery.

1.2 This policy is principally applicable to all employees of the Trust. However its principles also apply to anyone else who is given access to the Trust's ICT facilities: this may include employees of Essa Education, supply staff, directors and governors, other volunteers, contractors and visitors and actions to be taken by or against employees below should be read as applicable to any other persons given such access.

1.3 ICT is provided to support and improve the teaching and learning within Essa Foundation Academies Trust as well as ensuring the smooth operation of the Trust's administrative and financial systems.

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

1.5 The policy also provides advice and guidance to the Trust's employees on the safe use of social media. The acceptable use of ICT will be covered during induction and ongoing training will be provided, as appropriate.

1.6 This policy provides rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools.

1.7 Formal consultation with the teacher unions and trade unions recognised by the Trust on this policy has taken place.

1.8 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. A breach of this policy may result in action being taken against a director or governor in line with the Code of Practice for Members, Directors, and Governors.

2. Scope and purpose

2.1 This policy applies to all employees and to anyone else given access to the Trust's ICT facilities as set out above. Ensuring ICT is used correctly and properly and that inappropriate use is avoided is the responsibility of every employee and anyone else given access. If you are unsure about any matter or issue relating to this policy you should speak to the Trust's line manager, ICT manager or a senior member of staff.

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 and children 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. If we are required to investigate a breach of this policy you will be required to share relevant password and login details.

2.5 If you reasonably believe that a colleague has breached this policy you should report it without delay to the Trust's line manager or a senior member of staff.

3. Monitoring

3.1 The contents of the Trust's ICT resources and communications systems are the Trust's property. Therefore, employees should have no expectation of privacy in any message, files, data, document, 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 the Trust's electronic information and communications systems. Do not use the Trust's ICT resources and communications systems for any matter that you wish to be kept private or confidential.

3.2 The Trust reserves the right to monitor, intercept and review, without notice, employee activities using the Trust's ICT resources and communications systems, including but not limited to social media postings and activities, to ensure that the Trust's rules are being complied with and are being used for legitimate business purposes. As the Trust's employee you consent to such monitoring by your acknowledgement of this policy and your continued use of such resources and systems.

3.3 The Trust 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.

4. Policy rules

4.1 In using the Trust's ICT resources, the following rules should be adhered to. For advice and guidance on these rules and how to ensure compliance with them, you should contact the ICT manager.

4.2 **The network and appropriate use of equipment**

(a) You are permitted to adjust computer settings for comfort and ease of use, but these must be adjusted back after use for the next user.

(b) Computer hardware has been provided for use by employees and nursery children/pupils/ students and is positioned in specific areas. If there is a problem with any equipment or you feel it would be better sited in another position to suit the Trust's needs, please contact a member of ICT. Only the ICT manager/ICT team member will be allowed to move or adjust network equipment.

(c) Do not disclose the Trust's login username and password to anyone (unless directed to do so by a senior manager for monitoring or other purposes.

(d) You are required to change the Trust's password every half term in accordance with the login prompts. Ensure that you create appropriate passwords as directed. Do not write passwords down where they could be used by another individual.

(e) Do not allow nursery children/ pupils/ students to access or use the Trust's personal logon rights to any nursery/academy system, such as: Progresso, Apple ID's, or network resources. Nursery children/ pupils/ students are not permitted these access rights as it could lead to a breach of Data Protection and network security. Allowing nursery children/

pupils/ students such access could put you at risk if the Trust's accounts are used.

(f) Before leaving a computer, you must log off the network or lock the computer, checking that the logging off procedure is complete before you leave. Avoid leaving your device in a public area accessible by children/pupils/students such as the restaurant, library or strand areas. If family members access your devices ensure confidentiality is not breached. Ensure confidential documents are password protected.

(g) Ensure devices linked to the network are switched off when not in use.

(h) Only software provided by the network may be run on the computers. You are not permitted to import or download applications or games from the internet.

(i) You must not use any removable storage devices (RSDs), such as USB pens where you are unsure of the content or origin.

(j) Nursery child/pupil/student or staff data, or any other confidential information should only be stored on encrypted RSDs and not taken off the premises unless it has been encrypted to ensure data protection and confidentiality.

(k) RSDs should only be used for Trust purposes, outside of the Trust's premises where they are encrypted or have appropriate password protections.

4.3 **Mobile devices and laptop use**

The following rules are for use of any laptop, electronic tablets, mobile phone or other mobile device including those provided by the Trust. Referred to as mobile device(s):

(a) Access to the Trust's wireless network must be approved by the ICT manager. Personal devices must not connect to any network other than the guest network. Visitors will only be permitted on the guest network.

(b) You must ensure that the Trust's mobile device is password protected. This is essential if you are taking the mobile device off the Trust's premises.

(c) You must not leave your mobile device in an unsafe place, for example in your car.

(d) Mobile devices not provided by the Trust must have up to date anti-virus installed before being connected to the network and must be checked by the ICT team.

(e) You must ensure you have the appropriate permissions and security in place in order to access the Trust's network at home.

(f) All ICT kit must be returned to the ICT department directly should your employment cease with the Trust.

(g) You must ensure you are fully signed out of any accounts such as iCloud or personal E-Mail before leaving the Trust.

(h) All equipment must be returned in full in the event your employment with the Trust ceases.

4.4 **Internet safety**

(a) 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.

(b) Never give out personal information about a nursery child/pupil/ student or another employee over the internet without being sure that the request is valid and you have the permission to do so.

(c) Always alert the ICT manager/senior leader if you view content that makes you feel uncomfortable or you think is unsuitable. Remember that any personal accounts accessed on the Trust's network will be subject to monitoring.

(d) Always alert the ICT manager/senior leader if you receive any messages that make you feel uncomfortable or you think are unsuitable.

4.5 **Internet and email**

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

(b) Use of the internet at work must not interfere with the efficient running of the Trust. The Trust reserves the right to remove internet access to any employee at work.

(c) You must only access those services you have been given permission to use.

(d) You are required to check your work emails daily. Beware of fraudulent E-Mails and do not open attachments from unknown senders especially zip and exe files. If unsure seek advice from the ICT team.

(e) 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.

(f) Although the email system is provided for business purposes it is understood 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 the your work email account you should show the same care in terms of content as when sending work-related emails.

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

(h) 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.

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 /senior leadership.

(i) 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

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

(k) 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 manager/senior leadership.

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

(m) Do not use the computer network to gain unauthorised access to any other computer network, private user drives or protected secure network folders.

(n) Do not attempt to spread viruses.

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

(p) Never open attachments of files if you are unsure of their origin; delete these files or report to the ICT manager/senior leadership].

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

4.6 **Social networking and use of the chatrooms, community forums and messaging using any device**

The internet provides unique opportunities to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, Twitter, Linked In, blogs and wikis. Employees' use of social media can pose risks to the Trust's ability to safeguard children and young people, protect the Trust's confidential information and reputation, and can jeopardise the Trust's compliance with its legal obligations. This could also be the case during off duty time.

(a) You should exercise caution when using social networks. You should not communicate with nursery children/ pupils/ students over social network sites. You must block unwanted communications from nursery children/ pupils/ students. You are personally responsible for what you communicate on social media.

(b) You should never knowingly communicate with nursery children/ pupils/ students in these forums or via personal email account or personal mobile phones.

(c) You should not interact with any ex-pupil/ student of Essa Primary Academy or Essa Academy or an ex- nursery child of Essa Nursery who is under 18 on such sites.

(d) Communication with nursery children/ pupils/ students should only be conducted through the Trust's usual channels. This communication should only ever be related to the Trust's business.

(e) You must not post disparaging or defamatory statements about:

(i) Essa Foundation Academies Trust, its academies and Essa Nursery;

(ii) Essa Nursery's children or pupils/ students of EFAT academies, parents or carers;

(iii) the Trust's directors, governors or employees; or

(iv) other affiliates and stakeholders.

(f) You should avoid communications that might be misconstrued in a way that could damage the Trust's reputation, even indirectly.

(g) You should make it clear in social media postings that you are speaking on your own behalf. Write in the first person and use a personal email address when communicating via social media. Never set up personal accounts using work E-Mail addresses.

(h) If you disclose that you are an employee of Essa Foundation Academies Trust, you must also state that your views do not represent those of your employer. You should also ensure that your profile and any content you post are consistent with the professional image you present to nursery children/ pupils/ students and colleagues. Take care to avoid posting comments about Trust related topics even if you make it clear that the views do not represent the views of the Trust; your comments could still damage the Trust's reputation.

(i) If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you have discussed it with your manager **or the** ICT Manager.

(j) We recognise that employees may occasionally use social media for personal activities whilst at work. We authorise such occasional use so long as it does not involve unprofessional or inappropriate content and does not interfere with your role or your productivity. While using social media at work, circulating chain letters or other spam is never permitted.

(k) Circulating or posting commercial, personal, religious or political solicitations, or promotion of outside organisations unrelated to the Trust are also prohibited.

(l) Remember that what you publish might be available to be read by the masses (including the Trust, future employers and acquaintances) for a long time. Keep this in mind before you post content.

(m) If you see content in social media that disparages or reflects poorly on the Trust or the Trust's stakeholders, you should print out the content and contact the ICT Manager/ Principal/ or senior leadership team. All employees are responsible for protecting the Trust's reputation. Trust social media accounts should represent the views of the trust. Staff using social media accounts linked to the trust must adhere to the views and policies enforced by the trust and must not reflect their own personal views in any form.

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

(a) Violating copyright laws

(b) Attempting to harm minors in any way

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

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

(e) 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)

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

(g) 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.

(h) "Stalking" or otherwise harassing any user or employee

(i) Collection or storage of personal data about other users

5. Review of policy

5.1 This policy will be reviewed every 3 years, or earlier, if required by a change in legislation, by the Board of Directors and will be consulted on with the recognised teacher unions and trade unions.

5.2 The ICT Manager will monitor the application and outcomes of this policy to ensure it is working effectively and will report on this to the Board of Directors, LGBs, and the Nursery Management Committee, as required.

[redacted]

Employees of Essa Academy, Essa Primary Academy, and Support Services

ICT responsible user policy

Employee/ Supply Staff (print name):

Employee / Supply Staff Agreement:
I have read and understood this ICT responsible user policy.

I will use the computer network, internet and other new technologies in a responsible way in accordance with the rules set out in the policy.

I understand that network and internet access may be monitored.

I understand my obligations in relation to use of social media.

Signed:	**Date:**
Signed:	**Date:**

Directors and Governors, Other Volunteers, and Contractors with Access to the Trust's ICT Facilities

ICT responsible user policy

Name (print name):

Role:

Agreement:
I have read and understood this ICT responsible user policy.

I will use the computer network, internet and other new technologies in a responsible way in accordance with the rules set out in the policy.

I understand that network and internet access may be monitored.

I understand my obligations in relation to use of social media.

Signed:	**Date:**

Employees of Essa Nursery

ICT responsible user policy

Employee / Supply Staff Agreement:

I have read and understood this ICT responsible user policy.

I will use the computer network, internet and other new technologies in a responsible way in accordance with the rules set out in the policy.

I understand that network and internet access may be monitored.

I understand my obligations in relation to use of social media.

Signed: **Date:**