Electronic Inform ation and Communications System Policy

This policy is effective in all academies within the Learning without Limits Academy Trust

Associated policies
GDPR Privacy Notice for Pupils and Parents
GDPR Privacy Notice for Staff
GDPR Record of Processing Activities
GDPR Data Retention Policy
GDPR Freedom of Information Policy and Publication Schedule
GDPR Data Breach Policy
GDPR Data Protection Policy
GDPR Subject Access Request Policy

Version	Date	Author	Reason for change
V1.0	May 2018	DENE	Original Document
V2.0	September 2020	JOHE/ABEV	Version update with new roles and responsibilities

Introduction

The Trust's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff within the Trust who are required to familiarise themselves and comply with its contents. The Trust reserves the right to amend its content at any time.

This policy outlines the standards that the Trust requires all users of these systems to observe, the circumstances in which the Trust will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the General Data Protection Regulation (GDPR) and all data protection laws and guidance in force.

Staff are referred to the Trust's Data Protection Policy for further information. The School is also f required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications regul(1998

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- Audio and video streaming;
- Instant messaging;
- Chat rooms;
- Social networking sites; and
- Web mail (such as Hotmail or Yahoo).

No device or equipment should be attached to our systems without the prior approval of Trust network manager or Senior Leadership Team in the relevant academy. This includes, but is not limited to, any PDA or mobile phone, iPad (or other mobile device tablet), USB device, digital camera, MP3 player, infra red connection device or any other device.

The Trust monitors all e-mails passing through its systems for viruses. Staff should be cautious when opening e-mails from unknown external sources or where for any reason an e-mail appears suspicious (such as ending in '.exe'). Trust network manager should be informed immediately if a suspected virus is received. The Trust reserves the right to block access to attachments to e-mail for the purpose of effective use of the system and compliance with this policy. The Trust also reserves the right not to transmit any e-mail message.

Staff should not attempt to gain access to restricted areas of the neriiopef tuspip.6 (s)-2 ( )0.na36.9359 (

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the Trust's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) Transmitting a false and/or defamatory statement about any person or organisation;
(c) Sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive derogatory or may cause offence and embarrassment or harass others;
(d) Transmitting confidential information about the School and any of its staff, students or associated third parties;
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School;
(f) Downloading or disseminating material in breach of copyright;
(g) Copying, downloading, storing or running any software without the express prior authorisation of the Trust network manager;
(h) Engaging in on line chat rooms, instant messaging, social networking sites and on line gambling;
(i) Forwarding electronic chain letters and other materials;
(j) Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the exam