

Monitoring Policy

Name of Policy	MONITORING POLICY
Policy Level	Trust
Date of issue	October 2019
Author:	Trust Board
Date of Next Review:	October 2020
Signature	
Date of Signature:	16 TH December 2019

www.learningleading.org

01788 222060 | info@learningleading.org | @LearnLeadTrust

Address and Registered Office: 1 Bailey Road, Rugby CV23 0PD

Learning Today Leading Tomorrow is a company limited by guarantee. Registered in England and Wales No: 09027131. Tel: 01788 222060

Table of Contents

Introduction	3
Schedule of Responsibilities.....	3
Monitoring Use of Systems	4
CCTV.....	5
Principles behind the CCTV Policy	6
Procedures	6

Introduction

The Trust's Monitoring 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 at 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.

Schedule of Responsibilities

The CEO of Learning Today leading Tomorrow Trust (LT2) takes overall responsibility for the implementation of policies and procedures and to provide reports as appropriate to Trustees in relation to this policy.

Headteachers of LT2 schools and their Senior Leadership Teams will take active steps to promote good practice under this policy and review and monitor the management and implementation of this policy and practice in their School. They will identify training needs, ensuring competence in those staff who are responsible for and involved in the operation of this policy and associated guidance.

Teachers and other supervisory roles will, where required, conduct formal meetings, undertake relevant training in relation to this policy and ensure effective and competent operation of this policy.

All employees are required to cooperate fully and positively with the requirements of this Policy and to undertake any training recommended by their line manager.

The Trust's Head of Human Resources is responsible for providing advice and guidance under this policy and reviewing and updating the policy as required; ensuring continuing compliance in line with any developments in employment legislation, good employment practice and other LT2 policies. The Head of Human Resources may be requested to provide data for regular Trust Board HR reports where appropriate, providing confidential reports as required by the CEO and LT2 Trust Board on individual cases.

The following persons will generally be responsible for managing employees under this policy:

The School Headteacher (for School based teaching and educational or non-educational support staff) and the Chief Executive Officer (for School Headteachers and centrally appointed teaching and support staff) (the “Line Manager”).

Monitoring Use of Systems

The ICT systems, infrastructure and their contents are the property of the Trust and are provided to assist the performance of your work.

The Trust’s systems provide the capability to monitor telephone, e-mail, voicemail, web and other communications traffic. For business reasons, and in order to perform various legal obligations in connection with our role as a Trust and as an employer, use of the Trust’s systems including the telephone and computer systems, and any personal use of them, is electronically monitored from time to time. The Trust reserves the right to monitor and occasionally intercept network traffic on all aspects of its telephone and computer systems, whether stored or in transit, under its rights in the Regulation of Investigatory Powers Act (2000).

In accordance with the specific monitoring provisions contained in members of staff’s individual contracts of employment, monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for business purposes. Staff are referred to their individual contract of employment for further details.

Regular sweeps will be made of the ICT systems, including internet activity logs to check for inappropriate files or domain names. Where such files are located, further action as is necessary will be taken to ascertain the contents and if necessary to remove them. The Trust reserves the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (this list is non-exhaustive):

- (a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy; or
- (b) to find lost messages or to retrieve messages lost due to computer failure; or
- (c) to assist in the investigation a reasonable suspicion of breach of the law, this policy or another Trust policy; or
- (d) to comply with any legal obligation; or
- (e) To maintain operational effectiveness.

Users should be aware that second and third line ICT service staff with the appropriate privilege and when occasionally required to do so, will access all files stored on a computer or personal network folder. These staff will take all reasonable steps to maintain the privacy of users.

Proxy access to staff files including emails will only be given when authorisation is obtained from the Chief Executive Officer and Headteacher's. Such action will normally only be granted in the following circumstances:

- A suspected breach of the law or serious breach of this or another Trust policy
- At the lawful request of a law enforcement agency e.g. the police or security services

CCTV

All members of staff should be aware that the Trust uses [24 hour] CCTV surveillance in its premises for the prevention and detection of crime. The CCTV may be used for the protection of students, staff, visitors and Trust property.

Cameras are sited appropriately at each School and the extent of their field of view does not extend beyond the bounds of each school property

It is important that all staff understand that whilst on the premises, you may be recorded from time to time on surveillance video-tape and that you have consented to this. There are however, strict security controls over this recorded data and under normal circumstances no such data will be retained for longer than 7 days. Any question about data held in this way should be addressed to the Line Manager in the first instance.

All requests to view camera footage are logged and approval is granted only where the request is clearly in line with the purpose of using CCTV systems set out in this policy. External requests to access camera footage i.e. from the Police will only be approved where the appropriate legal platform for the request is cited and appropriately documented.

If disciplinary action results from information gathered through monitoring, the member of staff will be given the opportunity to see or hear the information in advance of the disciplinary hearing and to make representations about it.

In terms of CCTV system, this policy applies to the entire Learning Today Leading Tomorrow community; trustees, directors, governors, staff, students, parents and carers and anyone seeking to become a member of that community.

Principles behind the CCTV Policy

Learning Today Leading Tomorrow Trust operates all of its premises in accordance with UK law. The Trust's CCTV systems comply with the Information Commissioners Office document "In the picture: a data protection code of practice for surveillance cameras and personal information"

(<https://ico.org.uk/media/fororganisations/documents/1542/cctv-code-of-practice.pdf>).

Learning Today Leading Tomorrow is committed to the safety of staff, students, parents and visitors on all its premises.

As a public body Learning Today Leading Tomorrow has a duty to protect assets purchased by UK taxpayers.

Procedures

All premises using CCTV will display signage to indicate the presence of the CCTV system in accordance with the code of practice. This signage should identify the Trust as the body to whom Subject Access requests are to be made and provide a postal and email address to receive such requests.

Each School in the Trust will record all requests to view CCTV footage including the identity of the requester, the date of request and the outcome of the approval process including the date of disclosure of footage where approved. The requests must be forwarded to the relevant school principal for approval.

Requests from external organisations will be recorded as Subject Access Requests above but will also include a statement of the legal platform on which the request has been made and the appropriate documentation backing the request.

Subject Access requests made under the Data Protection Act 2018 by members of the public, parents or staff must be recorded and forwarded to the Data Protection Champion (See the Data Protection Policy). The date, time, location of the requested footage and identity of the requester must be recorded as well as a full record of the request made (i.e. letter or email received).

Footage exported from the CCTV system for any purpose other than for handover to the Police must be reviewed to ensure that the rights of those depicted in the footage are protected. If there is any doubt such cases must be referred promptly to the IT Services Manager.

Any footage extracted from the system must be signed out to the requester and must be tracked until it is returned and destroyed. The exception to this is any footage handed to the Police who are responsible for the footage from the point of handover

The retention period of footage from all Trust CCTV systems is 14 days. After this time footage will be deleted. Footage related to incidents under investigation may be retained until the investigation is completed and any follow up action is complete after which it must be deleted.

The request log for each School and the retention practices will be reviewed at least quarterly by the Trust Data Protection Officer and representatives of the School to ensure the validity of approvals to review footage