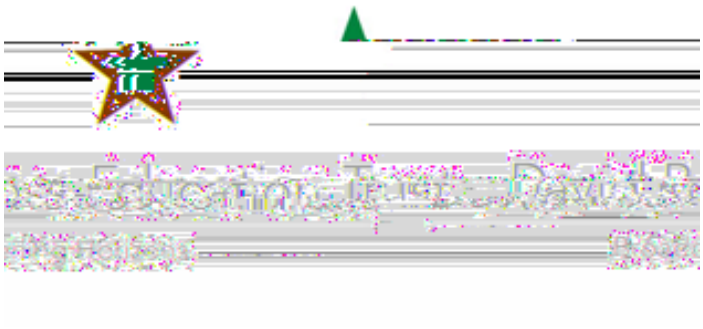

CCTV Monitoring Policy

Contents

1. Introduction

1.1. The David Ross Educations Trust aims to ensure that all personal data is collected, stored, and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018, as well as ensuring compliance with with the Information /2YYλăăλ2yŜŊŊă hŦŦλŎŜ //¢± /2ŘŜ 2Ŧ tŊl·ŐűλŎŜφ

1.2. The legislation concerning CCTV in s.29-31 of the Protection of Freedoms Act 2012 has produced a CCTV Code of Practice. The Trust, in managing its CCTV operations under this Code of practice will endorse and comply with all 12 guiding principles of the Surveillance Camera Code of Practice found in Appendix 2.

1.3. The majority of surveillance systems, such as Closed-Circuit Television (CCTV), are used to monitor or record the activities of individuals. As such, űKŜè ǈŊ2ŎŜăă λyŘλØλŘdzl·ŧăŊ information - their personal data.

1.4. The purpose of this policy is to define how the Trust uses Closed Circuit Television (CCTV) and its associated technology in monitoring both the internal and external environment of the Academy premises.

2. Policy Scope

2.1. This policy applies to all DRET offices, academies and transport where CCTV is in operation and is applicable to all staff, students and third parties (where appropriate). It also applies to temporary staff, contractors / installers and visitors.

2.2. ¢KŜ ¢ŊdzăűŊă Head Office and each Academy is responsible for operating their own CCTV system and ensuring it is compatible with this policy.

2.3. The use of, or extent of CCTV coverage is not mandated in this policy. The use or coverage is determined by individual Academy management. Individual Academies will bear the costs of installation and support of the system.

3. Why we use CCTV to Collect Personal Information

3.1. A critical component of a comprehensive security programme is the use of CCTV. Its use will be conducted in a professional, ethical, and legal manner.

3.2. CCTV monitoring is used by the TrustŊs Head Office and its Academies to:

- Deter and assist in protecting the Trust estate, learning community and property.
- Increase and enhance the wellbeing and personal safety of staff, students, and visitors, by reducing the fear of physical abuse, bullying, intimidation and crime.
- Assist in the overall management of the building and its facilities on a day-to-day basis.
- Further support law enforcement in a bid to deter and detect crime by assisting in reducing the incidence of crime and anti-social behaviour, including the identifying, apprehending, and prosecuting of any offenders on Academy sites.
- Protect members of the public and personal/private property, as well as promoting the Health and Safety of those within the Academy environment.

Used in cases where disciplinary matters arise.

password and the user should always lock the screens when not in use, in accordance with the Trust's Acceptable Use Policy. Exceptions to this may be authorised to allow out of hours access on a case-by-case basis. When this is authorised access will be restricted to a Trust laptop or mobile phone and authorised only by the DPO.

6.5. Any planned CCTV equipment to be purchased, must be done through normal IT Equipment purchasing processes to ensure cyber security awareness is considered and equipment linking in with the Trust's IT Architecture is considered.

7. Privacy

7.1. CCTV monitoring of public areas for security purposes on behalf of the Trust is limited to uses that do not violate the reasonable expectation of privacy as defined by the law.

7.2. Covert surveillance may be carried out in cases of suspected specific potentially criminal activity only where the objective of making the recording would be seriously prejudiced should the individual(s)

To inform the DPO of any requests for CCTV.

To ensure images of Data Subjects are redacted as required prior to release with support from the Trust It team where required.

Data Champion point of contact for any Subject Access Requests.

13.2 CCTV Operators/Site Team

Keep the system secure and operate within the constraints of this policy.

To provide access to footage as authorised in accordance with data protection mandated timelines.

Manage the day-to-day use of the system and liaise with suppliers and the IT team

Planning and implementation of CCTV systems and signage.

Liaising with the IT Team as Budget Holders on any associated costs.

Ensuring any procurement of new CCTV equipment is in liaison with the IT Team.

13.3 Academy IT Team

Provide support to CCTV operators.

Generating efficiencies by using chosen suppliers, providers, and equipment.

13.4 DPO

To be consulted over Subject Access Requests and authorise the release of any CCTV imagery.

14. Reporting and Consequences of Non-Compliance

14.1 Non-compliance with this policy may result in disciplinary action.

15. Policy Status