University of Kent CCTV Policy 2019

CONTENTS

CLAUSE

1. INTRODUCTION

1.1 The University is the owner and operator of the CCTV and Surveillance Systems on its campuses at Canterbury and Medway.

1.2 This document details the operating policy and standards for the use and operation of surveillance and management of CCTV and Surveillance Systems installed at the University of Kent Canterbury and Medway campuses.

1.3 The University believes that CCTV and Surveillance Systems have a legitimate role to play in helping to maintain a safe and secure environment for all students, staff and visitors. However, the University recognises that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address those concerns. Images captured on CCTV and Surveillance Systems are Personal Data, which must be processed in accordance with data protection laws. The University is committed to complying with its legal obligations and ensuring that the legal rights of students, staff and visitors are recognised and respected.

2. DEFINITIONS

2.1 In this policy, the following terms have the following meanings:

CCTV: means fixed position, domed, pan, tilt and zoom (PTZ) cameras at both internal and external locations designed to capture and record images of individuals and property.

Data: is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include audio recordings or static pictures such as printed screen shots.

Data Subjects: means all living individuals about whom the University holds Personal Data as a result of the operation of its CCTV (or other Surveillance Systems).

Personal Data: means Data relating to a living individual who can be identified from that Data (or other Data in the University's possession). This will include video images of identifiable individuals.

PIA: privacy impact assessment

Processing: is any activity which involves the use of Personal Data. It includes obtaining, recording or holding Personal Data, or carrying out any operation on Personal Data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring Personal Data to third parties.

Surveillance Systems: means any devices or systems designed to monitor or record images and, in certain cases, audio of individuals or information relating to individuals. The term includes CCTV as well as automatic number plate recognition (ANPR), body worn cameras, and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

University: The University of Kent, incorporated by Royal Charter with number RC000656 of The Registry, the University of Kent, Canterbury, Kent, CT2 7NZ.

3. ABOUT THIS POLICY

3.1 The University currently uses CCTV cameras and Surveillance Systems to view and record individuals on and around its campuses. This policy outlines: why the University uses CCTV and Surveillance Systems: how the University will use CCTV and Surveillance Systems; how the University will process data recorded by CCTV and Surveillance Systems to ensure the University is compliant with data protection laws and best practice, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 and the Human Rights Act 1998. This policy also explains how to make a subject access request in respect of Personal Data created by CCTV and Surveillance Systems.

3.2 The University recognises that information that the University holds about individuals is subject to data protection legislation. The images of individuals recorded by CCTV are Personal Data and therefore subject to the legislation. The University is committed to complying with all its legal obligations and seeks to comply with best practice suggestions from the Information Commissioner's Office.

3.3 The University strives to be a best practice CCTV operator and adopts the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 on a voluntary basis.

3.4 This policy covers all students, staff, employees, consultants, contractors, freelancers, volunteers, interns, casual workers, zero hours' workers and agency workers and visiting members of the public.

3.5 This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. The University may amend this policy at any time without consultation. The policy will be regularly reviewed to ensure that it meets legal requirements, relevant guidance published by the ICO and industry standards.

3.6 A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4. PERSONNEL RESPONSIBLE

4.1 The University has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the University's Head of Security.

4.2 The University's Head of Security may consult the University's Data Protection Officer at any time in relation to the Processing of Personal Data and the use of CCTV and Surveillance Systems.

4.3 Day-to-day operational responsibility for CCTV and Surveillance Systems and the storage of Data recorded is the responsibility of the Head of Security who is the operator of the Surveillance Systems and the Operational Manager for the purpose of this policy.

4.4 Responsibility for keeping this policy up to date has been delegated to the University's Head of Security and Data Protection Officer.

5. PURPOSES AND OBJECTIVES OF SURVEILLANCE SYSTEMS

5.1 The University currently uses Surveillance Systems for the purposes and objectives outlined below. Such use is necessary for the University's legitimate business purposes, including:

(a) Ensuring the safety of staff, students and visitors and to act as a deterrent against crime;

(b) To prevent crime and protect buildings and assets from damage, disruption, or vandalism;

(c) Assist in deterring, investigating and detecting crime or reports of possible crime;

(d) Facilitate the identification, investigation, apprehension and prosecution of offenders or suspected offenders;

(e) Support law enforcement bodies in the prevention, detection, investigation and prosecution of crime;

(f) Support the investigation of safety and security-related incidents and suspected misconduct by staff, students or visitors;

(g) Provide law enforcement bodies or the University with evidence which may lead to possible criminal, civil or disciplinary action against either staff, students or visitors or to investigate the possibility of any possible criminal, civil or disciplinary action against either staff, students or visitors;

(h) Provide evidential material for use in potential criminal, civil or disciplinary actions including employment tribunal proceedings;

(i) Facilitate the identification and investigation of any suspected breaches by the University or staff of their respective obligations and rights in connection with employment;

(j) Assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings; and

(k) To monitor traffic management, including monitoring parked vehicles, facilitating car parking and enforcement of the University's traffic policies, rules and regulations.

This list is not exhaustive and other purposes may be or become relevant.

5.2 The Surveillance Systems have been installed to provide:

(a) Images; and

(b) In respect of the Security & Transport public reception area only, images and audio

Which are suitable for the specified purposes for which they are installed, consistent with respect for individual privacy and in accordance with the CCTV Policy and Privacy Impact Assessment.

5.3 CCTV is checked daily by the Duty Control Room Operator to ensure that images remain fit for purpose and that the Data and time stamp recorded on images is accurate.

5.4 In the event of formal notification of any safety and security-related incidents and suspected misconduct complaints, any CCTV (with or without audio) or Body Warn Video (BWV) data connected to the incident will be retained and burnt to disc to secure and preserve evidence.

6. MONITORING

6.1 CCTV locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring. Surveillance Systems are located in different areas of the University campuses including, but not limited to, the following areas:

(a) Residences;

(b) Libraries;

(c) Food and drink outlets;

(d) Academic buildings;

(e) Open spaces;

(f) Car parks.

6.2 The primary monitoring facility for the Canterbury campus is located at the Security and Transport Centre security control room. The primary monitoring facility for the Medway campus is located in the Medway Security Office at the Medway Building.

6.3 Live viewing of CCTV on the Canterbury campus will ordinarily be through a feed into the security control room. CCTV is monitored in the security control room at the University's campus in Canterbury 24 hours a day, every day of the year.

6.4 Access to the security control room and primary monitoring facilities are limited to authorised personnel from the University's security staff and Estates department senior managers. Control Room Operators have unique and individual log in details and access is therefore controlled and audited on this basis.

6.5 A record of any viewing of or listening to recordings (visual or audio) captured by CCTV or Surveillance Systems will be maintained by security staff and will include a record of any persons viewing recordings, the time date and location of any recordings viewed and the purposes for which recordings are viewed.

6.6 The University shall ensure that live feeds from CCTV and Surveillance Systems are only viewed by authorised personnel from the University's security staff and Estates Department senior managers or members of staff approved by the Head of Security whose role requires them to have access to such Data. Recorded images will only be viewed or recorded audio data will be listened to in designated, secure offices and only be authorised personnel. This may include HR staff involved with disciplinary or grievance matters or who, with the express written consent of the HR Director, require access to the images in order to investigate suspected non-compliance by the University or member(s) of staff with their respective obligations and/or rights in connection with employment. Where any wrongdoing is suspected on the part of a member of staff, the recorded images may be disclosed to that staff member and/or an appropriate Trade Union or employee representative.

6.7 Images produced by CCTV and Surveillance Systems are as clear as possible in order that they are effective for the purpose for which they were intended. Audio data produced by CCTV and Surveillance Systems will provide a high enough quality of recording to achieve the stated purposes for which they were intended. CCTV and Surveillance Systems are subject to regular maintenance.

6.8 Staff using CCTV or Surveillance Systems are given appropriate training to ensure they understand and observe the legal requirements related to the Processing of relevant Data. Any misuse, or wrongful Processing, of the relevant Data could result in disciplinary action.

6.9 Appropriate signage will be displayed at entrances to the University's campuses and the entrances to buildings where CCTV or Surveillance Systems are installed so that individuals will be aware that they are entering an area, which is covered by CCTV, audio, or Surveillance Systems. Signs will:

(a) Be clearly visible, legible and be of a size appropriate to the circumstances;

(b) State the objectives of the Surveillance Systems; and

(c) Include the operator details and a contact telephone number for any enquiries.

7. USE OF DATA GATHERED BY CCTV

7.1 In order to ensure that the rights of individuals recorded by CCTV, audio or Surveillance Systems are protected, the University will ensure that Data gathered from CCTV, audio or Surveillance Systems are stored in a way that maintains integrity and security.

7.2 The Data generated by CCTV, audio and Surveillance Systems is stored on University servers. The University BWV camera data is stored using a cloud computing system. The University IS Dept. has ensured that all reasonable steps have been taken to maintain the security of its information

7.3 The University may engage any person or organisation to Process Data on its behalf and in accordance with its instructions (for example, a supplier which handles Data on its behalf or a control room or service engineer) to Process Data on its behalf. The University will ensure reasonable contractual safeguards are in place to protect the security and integrity of the Data.

8. RETENTION AND ERASURE OF DATA GATHERED BY CCTV

8.1 At the end of their useful life, all images and recordings stored in whatever format will be erased permanently and securely. Any physical matter such as tapes, discs, still photographs and hard copy prints will be disposed of as confidential waste.

8.2 Data recorded on or Surveillance Systems may be stored digitally either on hard discs or using a cloud computing system. Data from CCTV or Surveillance Systems will not be retained indefinitely but will be permanently deleted once there is no reason to retain the recorded information. Exactly how long images or audio will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, Data will be kept long enough only for incidents to become known. In all other cases, recorded images and audio will be kept for no longer than 28 days.

8.3 In certain circumstances in order to preserve recordings captured on CCTV, audio or Surveillance Systems, the Head of Security may direct that recordings captured on CCTV, audio or Surveillance Systems be transferred to CD (or another service medium) to achieve the purposes and objectives for which CCTV, audio or Surveillance Systems are installed. The transfer of any such recording to CD (or other service medium) will be processed by the duty security control room operator in the presence of a witness. Two copies will be made of any recordings transferred to CD (or other service medium) one of which will be held securely in the security control room and the other to achieve the purposes and objectives for which CCTV, audio or Surveillance Systems are processed. Any recordings transferred to CD (or other service medium) will be marked with indelible ink complete with the following information:

(a) Name and signature of the Control Room Operator burning the footage to CD;

(b) Name and signature of the person witnessing the process;

(c) Local disk reference number;

(d) Date the CD was created;

(e) Date, times and camera numbers of the footage included on the disk.

8.4 Copies made of any recordings captured on Surveillance Systems will be securely destroyed once there is no reason to retain the recorded information.

8.5 The Head of Security, or other nominated person, will ensure the forensic integrity of stored images. This includes providing law enforcement agencies with images of evidential quality, and ensuring that Data is retained, processed and the meta data (i.e. time, date and location) is correct.

9. USE OF ADDITIONAL SURVEILLANCE SYSTEMS

9.1 Prior to introducing any new Surveillance System, the University will carefully consider if they are appropriate by carrying out a Privacy Impact Assessment (PIA).

9.2 A PIA is intended to assist the University in deciding whether new Surveillance Systems are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

9.3 Any PIA will consider the nature of the problem that the University is seeking to address at that time and whether any Surveillance Systems are likely to be an effective solution, or whether a better solution exists. In particular, the University will consider the effect any Surveillance Systems will have on individuals and therefore whether the proposed use is a proportionate response to the problem identified.

9.4 No Surveillance Systems will be placed in areas where there is an expectation of privacy unless, in very exceptional circumstances, it is judged by the University to be necessary to deal with very serious concerns.

10. BODY WORN VIDEO CAMERAS

10.1 Body worn video cameras or mobile recording devices are used by campus security staff patrolling the campus and are designed to enhance the personal safety of staff responding to volatile situations or to record evidence or to promote safety on the University's campuses and to achieve the purposes and objectives for which Surveillance Systems are employed.

10.2 Body worn video cameras or mobile recording devices are clearly identifiable and any images or sound recorded are encrypted.

10.3 Body worn video cameras or mobile recording devices are only used in accordance with the stated purpose and objectives of this policy.

10.4 Staff issued with body worn video cameras or mobile recording devices will only initiate recording in response to suspected criminal activity, anti-social behaviour or disturbance, incidents where violence, aggression or threatening behaviour is displayed or where video evidence of a situation may be reasonably required to meet the purposes and objectives for which Surveillance Systems are deployed.

10.5 Prior to initiating any recording using a body worn video camera or mobile recording device, University staff will warn any persons being recorded or Data Subjects that video and sound recording is being initiated. Staff will record the date, time, location and reason for any recording made using a body worn video camera or mobile recording device.

10.6 Before being issued with a body worn video camera or mobile recording device operational staff will undergo training in the use of the device together with data protection law and best practice, the Protection of Freedoms Act 2012, the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 and the Human Rights Act 1998.

11. AUDIO

11.1 Audio recordings are not used at the University save as set out below.

11.2 In the Security & Transport Building public reception area, there have been incidents and/or conversations between staff and particular individuals where a reliable record was needed of what was said so it might be used as evidence in possible criminal or University misconduct/discipline investigations.

11.3 Other less privacy intrusive methods have been considered but these do not appropriately address the spontaneous or un-planned incidents or interactions requiring audio recording. Audio recording with CCTV recording may therefore be made within the Security & Transport Building public reception area for the purposes and objectives outlined in 5.1 above.

11.4 The Security & Transport Building public reception area is clearly identifiable, limited in area and has appropriate CCTV & audio recording signage. Any sound recorded provides a high enough quality of recording to achieve the stated aim and is encrypted.

11.5 The ICO recommendations concerning audio recording and 'Privacy by Design' for GDPR, have been incorporated within the Policy and operational applications:

(a) An existing PIA is in place.

(b) Audio Data collection will be limited as per Campus Security protocol.

(c) Security Control of the system is per this CCTV policy.

(d) Access Control of the data is per this CCTV policy.

(e) Process Monitoring is in place with quality assurance by Head/Deputy Head of Security and the University's Data Protection Officer (DPO).

(f) Continuous Evaluation into proportionality and necessity by the Head/Deputy Head of Security and the University's DPO.

11.6 The default state of audio recording will be "OFF" with normal visual CCTV in general operation. There is an independent switch to activate audio recording. The audio recording will only be activated for as long as necessary to discharge the Purposes and Objectives in 5.1 to mitigate the potential risk of recording excessive amounts of information. Once the necessity has passed to audio record the incident or interaction, the audio recording button will immediately be switched to the "OFF" position.

11.7 There is a visible warning sign to all staff or visitors within the non-public side of the public reception area that automatically lights up in red stating the word, "RECORDING" when the audio recording button has been activated to minimise collateral intrusion into the individual's privacy.

11.8 Security and Transport staff will only initiate audio recording in response to suspected criminal activity, anti-social behaviour or disturbance, incidents where violence, aggression or threatening behaviour is displayed or where video evidence of a situation in the Security and Transport public reception area may be reasonably required to meet the purposes and objectives for which Surveillance Systems are deployed.

11.9 The audio recording is automatically uploaded to University servers and retained for 28 days. At the expiration of 28 days, any recording including audio and BWV not downloaded for use pursuant to this policy is automatically deleted in accordance with the Data Protection Act 1998.

12. COVERT MONITORING

12.1 The University will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, the University reasonably believes there is no less intrusive way to tackle the issue.

12.2 In the unlikely event that covert monitoring is considered to be justified, it will only be carried out following a PIA with the express authorisation of the University's Director of Estates or in his/her absence the Deputy Director of Estates. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent students, staff and visitors will always be a primary consideration in

reaching any such decision. Where any covert monitoring includes the monitoring of a staff member, such monitoring shall not be conducted without the express written consent of the Director of HR.

12.3 Only limited numbers of people will be involved in any covert monitoring.

12.4 Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12.5 Where use of covert monitoring relates to a member of staff, the Head of Security will review the Legality, Proportionality, Audit trail, Necessity and Ethical justification with the Deputy Director Estates (Campus Services) plus the Head of HR before requesting authority from the Director of Estates to conduct covert monitoring.

12.6 Where covert monitoring is to be installed the senior manager responsible for any part or area of the University's campuses where a covert monitoring device is to be located will be consulted prior to the positioning of any covert monitoring device (unless that individual is to be the subject of any covert monitoring).

13. REQUESTS FOR DISCLOSURE

13.1 The University may share Data with other organisations, for example with the police or law enforcement agencies, where it considers that this is reasonably necessary for the purposes and objectives set out in paragraph 5 of this policy.

13.2 No images from the University's CCTV or Surveillance Systems or audio will be disclosed to any third party, without express permission being given by the Head of Security. Data will not normally be released unless satisfactory evidence that it is required for legal proceedings or a court order from a court with competent jurisdiction has been produced.

13.3 In other appropriate circumstances, the University may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

13.4 The University's Head of Security will maintain a record of all disclosures of recordings made on CCTV, audio and Surveillance Systems.

13.5 Requests to access recorded images or audio for the purposes of reviewing footage to establish if any evidence has been captured on CCTV or Surveillance Systems will be restricted to University security staff, the Deputy Director Estates (Campus Services), professional legal advisors and the police or other relevant law enforcement agency where appropriate.

13.6 Requests to access recorded images or audio under paragraph 13.5 of this policy should be made by the University manager and /or HR Manager responsible for the relevant investigation or hearing only, and will be authorised by the University's Head of Security. In this context, "investigation" refers to both formal and informal investigatory processes which may be initiated by the University from time to time. Any such request will be accompanied by a statement from the responsible manager confirming whether the images will (or may) require disclosure to a Trade Union or employee representative.

13.7 Before disclosing any Personal Data in response to a request made to access recorded images or audio under paragraph 13.5 above, the University's Head of Security will be satisfied that the request is compatible with the stated purposes and objectives as stated in paragraph 5 of this policy and the necessary Data Subject Access Request form has been correctly completed and submitted. Where necessary, the University's Head of Security will consult with the University's HR Director and Data Protection Officer (and if needed professional legal advisors) in order to determine whether it is appropriate to grant any requested disclosure.

13.8 Where any request made pursuant to paragraph 13.5 of this policy is authorised by the University's Head of Security, copies of any recordings captured on CCTV or Surveillance Systems will be transferred to CD (or another service medium) to achieve the purposes and objectives for which the request was made and will be signed for by the authorised University Manager and or HR Manager. Copies made of any recordings captured on CCTV or Surveillance Systems will be securely destroyed once there is no reason to retain the recorded information.

13.9 If the Head of Security is unavailable, the Deputy Head of Security or nominated appointee from the Estates Senior Management Team are authorised to carry out the same functions as the Head of Security.

14. SUBJECT ACCESS & FREEDOM OF INFORMATION ACT REQUESTS

14.1 Data Subjects may make a request for disclosure of Personal Data which may include CCTV images including audio where appropriate (a "**Data Subject Access Request**"). A Data Subject Access Request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with the University's subject access policy at *https://www.kent.ac.uk/infocompliance/dp/access-requests.html*

14.2 In order for the University to locate relevant footage/recordings, any requests for copies of recorded images or audio must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the Data Subject.

14.3 The University reserves the right to obscure images and/or edit audio of third parties when disclosing recordings captured on CCTV or Surveillance Systems when responding to a Data Subject Access Request once the technology is available at the University.

14.4 Any request for recorded images or audio other than by way of a Data Subject Access Request will be considered under the Freedom of Information Act 2000 (an "**FOIA Request**"). An FOIA Request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with the University's policy at *https://www.kent.ac.uk/infocompliance/foi/request.html*

14.5 On receipt of a Data Subject Access Request or FOIA Request, the University Data Protection Officer shall advise the University's Head of Security whether any disclosure should be made.

15. MONITORING AND COMPLIANCE

15.1 An annual Privacy Impact Assessment (PIA) will be conducted by the University Head of Security to evaluate the effectiveness and justification for the continued use of CCTV and Surveillance Systems in use at the University and assess compliance with data protection laws and the CCTV Code of

Practice issued by the Information Commissioner's Office. The Head of Security will consult the Data Protection Officer when conducting a PIA. The results of the PIA will be assessed against the purpose and objectives set out in paragraph 5 of this policy.

15.2 The University's CCTV and Surveillance Systems are the subject of a PIA. The University will annually publish a PIA on the University's security department webpages. Undertaking a PIA allows the University to continually assess whether there is a pressing need for CCTV and Surveillance Systems and whether CCTV and Surveillance Systems in operation are a proportionate response.

15.3 The University's Deputy Head of Security or Security Duty Manager will access random footage of recorded images or audio at least once every 28 days to monitor compliance with this Policy, the Data Protection Act and the Information Commissioner's Code of Practice. These checks will be recorded and will also include checks to ensure the processes and procedures contained in this policy are being adhered to.

15.4 At the start of each shift, the Duty Control Room Operator will complete and record a check on the operational status of the CCTV and Surveillance Systems to include:

(a) Verifying that the time and date stamp on recorded images is accurate;

(b) Verifying that all cameras are recording correctly and are fully serviceable, reporting defects without delay;

(c) Establish that the quality of images being recorded is suitable for the specified purposes and objectives for which they are installed set out in paragraph 5 of this policy.

16. ONGOING REVIEW OF CCTV USE

The University will ensure that the ongoing use of existing CCTV and Surveillance Systems is reviewed at least every 12 months to ensure that use remains necessary and appropriate, and that any Surveillance System is continuing to address the needs that justified its introduction.

17. COMPLAINTS

Section A - Complaints relating to CCTV or Surveillance Systems

17.1 Any complaints relating to CCTV including audio CCTV or Surveillance Systems should be directed in writing in the first instance to the University's Head of Security at the following address:

Head of Security, Security and Transport Centre, University of Kent, Canterbury, Kent, CT2 7NQ.

17.2 Once a complaint has been received in writing, the University's Head of Security will respond to the complaint within 28 days. Records of all complaints regarding the CCTV, audio or Surveillance Systems together with any follow up action will be maintained by the University's security department.

17.3 If a person making a complaint is still unsatisfied with the response given, if the complainant is a member of staff or a former or current student at the University, they should use the University's formal

grievance procedures. In all other cases, any appeal should be made to the University's Director of Estates.

Section B - Complaints relating to the Processing of Personal Data

17.4 Any complaint relating to the Processing of Personal Data should be directed in writing to the University Data Protection Officer at the following address:

University Data Protection Officer, Information Compliance, Darwin College, University of Kent, Canterbury, Kent, CT2 7NY.

17.5 Once a complaint has been received in writing, the University's Data Protection Officer will respond to the complaint within 28 days. Records of all complaints regarding the CCTV or Surveillance Systems together with any follow up action will be maintained by the University's security department and Information Compliance Team.

17.6 If a complainant is unsatisfied with any response issued under paragraph 17.5 they may refer their complaint to the Information Commissioner *https://ico.org.uk/*