Acceptable Usage Statement & Staff Privacy Notice

The following information covers the security and use of all The Sutton Academy information and IT equipment; whilst also explaining the use of any staff data held by the academy. It also includes the use of email, internet and mobile IT equipment. This information applies to all The Sutton Academy employees, contractors and agents (hereafter referred to as 'individuals').

Computer Access Control - Individual's Responsibility
Access to the academy IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently individuals are accountable for all actions on The Sutton Academy IT systems.

Individuals Must Not:
· Allow anyone else to use their user ID and password on any academy IT system.
· Leave their user accounts logged in at an unattended and unlocked computer.
· Use someone else's user ID and password to access academy IT systems.
· Leave their password unprotected (for example writing it down).
· Perform any unauthorised changes to academy IT systems or information.
· Attempt to access data that they are not authorised to use or access.
· Exceed the limits of their authorisation or specific business need to interrogate the system or data.
· Connect any non-academy authorised device to the academy network or IT systems.
· Store academy data on any non-authorised academy equipment.
· Give or transfer academy data or software to any person or organisation outside academy without the authority of academy.

Internet & Email - Conditions Of Use
Use of academy internet and email is intended for business use, and all individuals are accountable for their actions on the internet and email systems.

Working Off-Site
It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:
· Working away from the academy must be in line with academy remote access policy.
· Equipment and media taken off-site must not be left unattended in public places
· Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used on devices where data is stored locally and may be taken offsite.

Mobile Storage Devices
Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only academy authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Monitoring and Filtering
All data that is created and stored on academy computers is the property of academy and there is no official provision for individual data privacy, however wherever possible the academy will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this, or any other policy. The Sutton Academy has the right to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

Workforce Data
We, The Sutton Academy, are the Data Controller for the purposes of the GDPR. Personal data is held by the academy about those employed or otherwise engaged to work at the academy. This is to assist in the smooth running of the academy and/or enable individuals to be paid. The collection of this information will benefit both national and local users by:

- Improving the management of academy workforce;
- Enabling a comprehensive picture of the workforce and how it is deployed;
- Informing the development of recruitment and retention policies;
- Enabling ethnicity and disability monitoring; and
- Supporting the work of the Academy Teachers' Review Body.

This personal data includes some or all of the following - identifiers such as name and National Insurance Number and characteristics such as ethnic group; employment contract and remuneration details, qualifications and absence information.

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain academy workforce information to us or if you have a choice in this.

Who we share this information with
We routinely share this information with - The Local Authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the Academy Workforce) (England) Regulations 2007 and amendments.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to academy funding / expenditure and the assessment educational attainment.

We share personal data with Human Resource and Payroll purposes.

Data collection requirements
The DfE collects and processes personal data relating to those employed by the academy and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Student Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on

whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment.

To be granted access to academy workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information or for further information on Data Protection and the academy's GDPR compliance please contact the academy Data Protection Officer, Mr Paul Blakemore.