REDHILL ACADEMY TRUST
Exsisto Optimus

Data Acceptable Use Statement

Approving Body	Redhill Academy Trust Exec Board
Date Approved	May 2018
Version	V 1.0
Supersedes Version	-
Review Date	May 2021
Legislation	GDPR Act 2018
Further Information/Guidance	

ACCEPTABLE USE POLICY FOR DATA

All staff and working visitors should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfil its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). This Acceptable Use Policy has been created to ensure that all staff are aware of and follow specific rules.

1. Data to which this AUP applies

1.1 Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth).

1.2 Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an unauthorised individual. For example SEN, racial or medical data, bank details, phone numbers.

1.3 This AUP also applies to all confidential data.

2. Security of paper-based data

2.1 Staff are responsible for ensuring that data issued to them remains secure. On site this mean keeping data away from being easily accessible by unauthorised personnel e.g. students.

2.2 If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.

2.3 Data should never be taken outside of the EU.

2.4 Particularly sensitive data, e.g. SEN or medical records, payroll details etc., should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.

2.5 All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).

3. Security of electronic data

3.1 Ensure that your passwords for access to the network, email, SIMS etc. are strong passwords. You should change these on a regular basis, and not tell other members of staff or students your passwords.

3.2 Ensure that you lock or log out of your computer when leaving it unattended, even for a short period of time. You are responsible for activity that takes places using your credentials, which can be monitored by the school IT support team.

3.3 Ensure that on screen data is not visible to students or other unauthorised personnel.

3.4 Data must not be stored on staff laptops or any electronic device outside of school without being encrypted and must comply with the GDPR. Wherever possible taking data out of school should be avoided.

3.5 Use of USB memory devices is permitted, however these must be encrypted before any data from the school's system can be written to them. This encryption will be forced (Bitlocker to go).

3.6 Use of External Hard Drives is permitted, however, these must be encrypted before any data from the school's system can be written to them. (Bitlocker to go).

3.7 Use of Personal laptops is not permitted. The use of School Laptop outside of school is permitted, however, ALL devices must have encryption installed by the school ICT Support team, and this will either be BitLocker or Des Lock.

3.8 Prior to leaving the Trust employment staff must return all equipment provided by the school, personal laptops must be checked by ICT support to remove any private data.

3.9 Files should be deleted from the network, encrypted laptops, external hard drives and USB drives when the data is no longer required, in line with the school's data retention policy. When deleting a file from a USB drive outside of school you should use shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

3.10 When sending emails, any emails sent outside of the Trust Office 365 tenancy must not contain personal data. Any attachments that are sent must be password protected.

3.11 Photos and videos of students must only be taken using school owned devices. Any exception to this can only be authorised by the Head of School/Executive Headteacher for example, when on an educational visit following which, the photographs/videos must be transferred to a school device and deleted from the personal device. The placing of photos on websites and social media must only take place following the formal written consent of the student.

3.12 If you use your mobile device(s) to access school email or Office 365 you must make sure that the device is protected with a password or pass-code logon or some other form of physical authentication.

3.13 When your employment with the school terminates, your electronic accounts will be immediately disabled when your contract ends.

3.14 Should a data breach or a potential data breach occur, you must report this to the School Operations/Business Manager without delay.