DATA ACCEPTABLE USE POLICY

APPROVING BODY	Trust Audit Committee
DATE APPROVED	29/09/2021
VERSION	2.0
SUPERSEDES VERSION	1.0
REVIEW DATE	01/09/2024
LEGISLATION	• Data Protection Act (2018)
FURTHER INFORMATION/GUIDANCE	UK General Data Protection Regulation (UK GDPR)

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 academy. Failure to do so may result in disciplinary action.

It is vital that the academy 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.

Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Education (Independent School Standards) Regulations 2014
- The School Standards and Framework Act 1998

This policy will be implemented in conjunction with the following other Trust policies:

- Staff Code of Conduct Policy
- Academy E-Safety Policies
- UK GDPR Data Retention Policy
- Data Protection Policy
- Data Retention Policy
- Various Privacy Notices

1. Policy Statement

1.1 The Redhill Academy Trust (The Trust) provide data resources to facilitate a person's work as a student or employee within the Trust. The Trust seeks to provide a professional working environment for its students and staff. The Trust values its systems as important business and educational assets.

1.2 Wherever referred to 'The Trust' throughout this policy, includes employees in all individual Academies in the Trust, including the Teaching School Hub, The College, and the Central Support Teams.

1.3 The objectives of this policy are to ensure as far as is possible:

1.3.1 Trust data systems both electronic and non-electronic are as safe, secure and as effective as possible.

1.3.2 The Trust is protected from damage or liability resulting from the use of its facilities for purposes contrary to the law or any agreement under which the Trust or its systems operate.

1.4 This policy does not form part of any employee's contract of employment and it may be amended at any time.

2. Roles, Responsibilities and Implementation

2.1 The Trust Audit and Risk Committee has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework. The Committee delegates day-to-day responsibility for operating the policy and ensuring its implementation, review and maintenance to the Director of Operations and Academy Data Protection Leads.

2.2 Leaders and managers have a specific responsibility to ensure the fair application of this policy. All members of staff are responsible for supporting colleagues in ensuring its success.

2.3 All staff have a personal responsibility to ensure that they and others, who may be responsible to them, are aware of and comply with this policy and its guidelines. This includes staff who are working on-site or remotely.

2.4 The Trust will investigate all incidents involving the potential breach of this policy. Overall responsibility for investigation is with the Director of Operations, who will notify the appropriate managers. Incidents which are found to contravene this policy will be subject to disciplinary procedures.

3. Data to which this Policy applies

3.1 For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

3.2.1 race or ethnic origin;
3.2.2 political opinions;
3.2.3 religious or philosophical beliefs;
3.2.4 trade union membership;
3.2.5 physical or mental health;
3.2.6 an individual's sex life or sexual orientation;
3.2.7 genetic or biometric data for the purpose of uniquely identifying a natural person.

3.3 Special category personal data is given additional protection under the UK GDPR, and further safeguards apply where this information is to be collected and used.

3.4 The UK GDPR also gives additional protection to personal data relating to criminal convictions and offences or related security measures (including information about criminal activity, allegations or suspicions, investigations and proceedings) ("criminal offence data").

4. Security of paper-based data

4.1 Staff are responsible for ensuring that data issued to, or operated on by them, remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel.

4.2 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, when not in use.

4.3 Data should **never** be left unattended in a vehicle.

5. Data should **never** be taken outside of the EU.

5.1 Special Category Data, should **never** be removed from the academy site and must be stored in a secure area e.g. locked cupboard, filing cabinet or office at all times, when not in use. Special Category Data should never be left unattended.

5.2 Before sharing data, all staff members will ensure that:

- They are allowed to share it.
- Adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

5.3 All paper-based records containing data should be securely shredded, or confidential waste removal, when no longer of use. You should not keep records beyond their retention period.

5.4 Paper based records should be destroyed in compliance with the Trust Data Retention Policy

6. Security of electronic data

6.1 Ensure that your passwords for access to the network, email, MIS etc. are strong passwords, including at least one number, capital letter and special character. You should change these on a regular basis (at least annually), and never share passwords, or login details with other members of staff or students.

6.2 Access to all IT accounts for all IT systems are the sole responsibility of the named owner of the account.

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

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

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

6.6 Use of USB memory devices is permitted; however, these must be encrypted and will be supplied to you by the academy ICT support team on request. No personal USB devices may be used under any circumstances. This USB drive should remain physically secure both in transit and when stored. As a preferred alternative, remote access to the Academy Microsoft 365 system will be provided to all staff and should be used to access and transfer files wherever possible.

6.7 Use of External Hard Drives is permitted; however, encryption must be installed on the device by the school ICT support team prior to first use.

6.8 Use of both Personal and School Laptop's outside of school is permitted; however, ALL laptops must have encryption installed by the school ICT Support team, and this will either be BitLocker or Des Lock.

6.9 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 confidential data and the encryption.

6.10 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 Trust's data retention policy. When deleting a file from a USB drive outside of the academy you should use shift and delete to avoid the risk of a copy of the file being stored in the recycle bin.

6.11 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 or sent with confidential in the subject line, which will automatically encrypt the email.

6.12 Circular emails to parents and other agencies outside of the Trust are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

6.13 Photos and videos of students must only be taken using academy owned devices unless prior permission has been given by a member of the Senior Leadership Team.

The placing of photos on websites and social media must only take place following the formal written consent of the student. Consent must not be assumed.

6.14 If you use your mobile device(s) to access academy 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.

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

6.16 Academy Data Protection Leads are responsible for ensuring continuity and recovery measures are in place to ensure the security of protected data.

6.17 Should a data breach or a potential data breach occur, you must report this to the Operations/Business Manager without delay, and an internal investigation will be carried out.

7. Policy Review

7.1 This policy will be reviewed every three years or earlier if required by changes in legislation.