The Four Stones Multi Academy Trust
SIMS Parent App Acceptable Use Policy

Version Control
Policy authors: Ruth Allen & Rob Bick
Policy approved by: Finance, Audit and Risk Committee
Next policy review date: Summer 2022

Version	Date	Details
1.0	23rd June 2020	Re-written so that there is one policy for The Four Stones Multi Academy Trust

SIMS Parent App allows you, as parent/carer, to view key information about your son/daughter. The information that you have access to may be sensitive and/or personal and therefore we ask you to adhere to the following guidance in order to protect your son/daughter(s) information:

- Parents/carers will not share their password with anyone;
- Parents/carers will use a strong password. Please see password guidance section below;
- Parents/carers will not attempt to **amend or delete** data of their own children, another user or the school;
- Parents/carers will not use the SIMS Parent App for any illegal activity, including the violation of data privacy laws;
- Parents/carers will not publish information taken from SIMS Parent App elsewhere without permission;
- Parents/carers will not access data or any account owned by another user;
- Parents/carers who identify a security problem with SIMS Parent App must notify the school immediately, without demonstrating the problem to anyone else.

Password guidance

In order to ensure that your account remains secure your password must be a "strong" password, including at least eight characters, at least one symbol, at least one number, at least one lower case letter and at least one upper case letter. An example of a "strong" password would be **H4yBr!dg3.** If you have particular problems remembering passwords, one strategy is to choose a memorable phrase/word then substitute numbers and symbols for letters-e.g. **K1ngCh4r!35**. If you use a similar password when an old one expires, you must completely change the password after three changes. e.g. **K1ngCh4r!35.01** could be changed to **K1ngCh4r!35.02** and then **K1ngCh4r!35.03** but the "**K1ngCh4r!35**" section would have to be replaced on the fourth change.

Further advice

- Always log out, or "lock" the screen when leaving your device unattended.
- Don't write passwords down or leave them near devices;
- Don't save passwords in web browsers;
- Don't ever email your password or use it in an instant message;
- Always turn off your device using the "Shut Down" option;
- Be aware of people watching you as you enter passwords or view sensitive information;
- Don't use unsecured public wireless hotspots.