# Staff and Volunteer Acceptable Use

**Date: January 2018**

**Review: January 2019**

Continuing The Learning Journey Together

## Staff and Volunteer Acceptable Use Policy

**This Code of Conduct is intended to ensure that all members of staff are aware of the expectations that are placed upon them. It is intended to support staff in their role, promoting responsible practice, enabling staff to safeguard pupils and safeguard themselves. All school information systems, including all staff laptops are fitted with Forensic software. This is monitored by senior leaders on an ongoing basis. This is for the protection of all members of the school community.**

**Staff should ensure that they read and consult the school's e-safety policy and social media policy, for further information and clarification. Both are available on the website.**

### Learning and Teaching

- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

### School Information Systems

- I understand that the school will monitor my information systems and internet use to ensure policy compliance e.g. Forensic Software.
- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role. Staff are responsible for ensuring that they take full responsibility for the management of their school laptops and school systems.
- I will respect copyright and intellectual property rights.
- I understand that school information systems or equipment may not be used for private purposes, without specific permission from the Principal.

### Social Media and Social Networking

- Staff must not access personal social media during their directed working times.
- Staff must not post on personal social media during the school day.
- Staff must never post images taken on the school premises or during school activities/trips.
- Staff should never accept an invitation to 'friend' a pupil. Staff must not give their personal email addresses to any pupil or parent.
- Staff must not use any school systems for social networking purposes.
- All staff, should review their social networking sites to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the academy if they are published outside of the site.
- If as a member of staff, you become aware that images or content on social networking sites refer to you and the content could cause embarrassment or damage the reputation of the academy, you should seek to ensure that this is removed.
- Staff must ensure that their social media accounts are secure. Passwords must be kept securely and not passed on to anyone. You remain responsible for any content published on your social networking site.
- Confidentiality needs to be considered at all times, even after employment.
- Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.
- Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social

networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the academy or another academy, could result in formal action being taken against them.

- Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the academy or the Trust into disrepute.
- Employees should be careful not to join or be associated with any online groups which due to their content or objectives are incompatible with the policies and objectives of the academy.
- Some social media sites and other web-based sites have fields in the user profile for job title etc. Staff should not put any information onto the site that could identify either your profession or the academy where you work. In some circumstances this could damage the reputation of the academy, the profession or the Trust.
- There are no circumstances that will justify adults possessing indecent images of children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children, if proven.
- Staff should not use equipment belonging to the academy to access any indecent images; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

## Use of Mobile Phones

- Mobile phones should be out of sight and on silent at all times whilst on school premises. Personal mobile devices must not be used to take images of pupils. School cameras and ipads should be used for this purpose and images are to be safely stored on the school network system e.g staffshare.

## Data Protection

- I will ensure that I take responsibility for safeguarding pupil data by ensuring that school laptops, iPads, digital cameras etc. are kept secure at all times in order to prevent data protection breeches.
- I will not use personal data of any pupil, parent or colleague without the prior agreement of the principal. This includes entering pupil data on external online systems e.g. Class Dojo.
- I will respect system security and I will not deliberately disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without authorisation.
- I will adhere to policies and procedures that require personal data to be kept secure and used appropriately, whether in school, taken off the school premises or accessed remotely.

## Safeguarding.

- I will report any incidents of concern regarding children's safety to the school E-Safety Lead or the Designated Safeguarding Lead (DSL).

I have:

- been trained in using the school's information system at (an appropriate) level;
- read the school's e-safety policy and know who the ESL (Miss A James/ Miss N Dono) and DSL (Mrs G Frost) are;
- agreed to follow the school's policy and this Code of Conduct.

I further understand that the school may monitor the use of the school' s information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Staff are expected to report any breaches of the Code of Conduct to a member of the Senior Leadership team. Disciplinary procedures and policies will be followed should there be any breach of this Code of Conduct.

Print Name:

Signed:

Date: