Social Media Policy

St Michael's CofE Primary Academy considers the use of social media and social networking sites to be a strictly personal activity. The use of social networking applications has implications for our duty to safeguard children, young people, vulnerable adults and employees.

Related Document: E-safety Policy

1. Purpose:

The purpose of the policy is to ensure:

- All employees and students are safeguarded against allegations which may arise through inappropriate use of social media and networking sites.
- The reputation of the school and Employees is not adversely affected.
- The school is not exposed to legal and governance risks.
- To ensure all employees have signed an appropriate code of conduct in relation to acceptable use of school technology and social interaction.

2. Scope:

Social networking applications include but are not limited to:

- Bloggs for example 'Blogger'
- On-line discussion forums such as 'Ning'
- Collaborative spaces such as 'Wetpaint'
- Media sharing service such as 'Youtube'
- Micro-blogging applications such as 'Twitter'
- Facebook

Many of the principles of this policy also apply to other types of on-line presence such as virtual worlds.

3. Policy:

Employees are to be aware of the following:

- **Never** engage in social networking with a student. All electronic communications with students should be done via the school e-mail which can be regulated. To engage in social networking with students leaves employees vulnerable to accusation and speculation. Employees must take all steps necessary to safeguard themselves. Should

you suspect that a student seeks an inappropriate relationship with you, you must bring this to the attention of your line manager immediately.

- Employees are **strongly advised** not to enter into social networking with former students. Circumstances may lead employees to be vulnerable to accusation and speculation.
- Be aware that by identifying yourself as a member of St George's CE Academy Newtown you become, to some extent, a representative of the school and everything you post has the potential to reflect on the school and its image. Therefore, should employees identify themselves as school members they take on the responsibility for representing the school in a professional and positive manner. Defamatory statements about the school or colleagues can lead to disciplinary action or even lawsuits.
- Employees should **never** name students or make reference to a student's **personal circumstances**. Safeguarding / child protection breaches can easily be made by the use of an innocent or thoughtless comment.
- Employees should be aware that social networking sites have varying levels of security and as public sites all are vulnerable to breaches in security.

4. Guidance

Employees are asked to take special attention of the "Guidance for Safe-Working Practice for adults working with Children and Young People" - paragraphs 12 (Communication with Children and Young people ~ including the Use of Technology) and 13 (Social Contact). These are shown below:

Paragraph 12 - Communication with Children and Young People (including the Use of Technology).

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based websites.

Internal e-mail systems should only be used in accordance with the organisation's policy.

Paragraph 13 - Social Contact

Adults who work with children and young people should not seek to have social contact with them or their families, unless the reason for this contact has been firmly established and agreed with senior managers, or where an adult does not work for an organisation, the parent or carers. If a child or parent seeks to establish social contact, or if this occurs coincidentally, the adult should exercise her/his professional judgement in making a response but should always discuss the situation with their manager or with the parent of the child or young person. Adults should be aware that social contact in certain situations can be misconstrued as grooming.

Where social contact is an integral part of work duties, e.g. pastoral work in the community, care should be taken to maintain appropriate personal and professional boundaries. This also applies to social contacts made through interests outside of work or through the adult's own family or personal networks.

It is recognised that some adults may support a parent who may be in particular difficulty. Care needs to be exercised in those situations where the parent comes to depend upon the adult for support outside their professional role. This situation should be discussed with senior management and where necessary referrals made to the appropriate support agency.

5. Discipline

Breaches of this policy would be investigated under the Disciplinary policy and may result in disciplinary action being taken. Staff are required to sign the attached code of conduct in relation to social interaction and the use of school IT equipment and technology.

Appendix: Staff Information Systems Code of Conduct

To ensure that all members of staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the academy's e-safety policy and Social Media and Social Networking Policy for further information and clarification.

- The information systems are Academy property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

I agree that:

- I will ensure that my information systems use will always be compatible with my professional role. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

  - I will not use or share my personal (home accounts /data (eg Facebook, email, ebay etc) with pupils.

  - I will only use the school's e-mail / Internet / Intranet / Learning Platform and any related technologies for professional purposes only (unless permission has been obtained from an appropriate line manager).

  - I understand that academy information systems may not be used for private purposes.

  - I understand that the academy may monitor my information systems and Internet use to ensure policy compliance.

  - I will respect system security and I will set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).

  - I will ensure that personal data is kept, used, moved and shared securely and is used appropriately, whether in academy, taken off the academy premises or accessed remotely by only using password protected encrypted USB pens on computers purchased by academy. Personal computers will never be used for work purposes.

  - I will ensure the laptop provided for me by academy is returned to the ICT technician on a termly basis so necessary updates and checks can be run.

  - I will respect copyright and intellectual property rights.

  - I will report any incidents of concern regarding children's safety and unsuitable content and/or ICT misuse to the named e-Safety officer or the Designated Child Protection Coordinator.

  - 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.

  - I will only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.

- I will only give permission to pupils to communicate online with trusted users.
- I will use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- I will not install any software or hardware on equipment belonging to the school.
- I will not visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - pornography (including child pornography)
    - promoting discrimination of any kind
    - promoting violence or bullying
    - promoting racial or religious hatred
    - promoting illegal acts
- I will not breach any Local Authority/Academy policies, e.g. gambling
- I will not do anything which exposes others to danger
- I will not use any other information which may be offensive to others
- I will not forward chain letters
- I will not use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff.

I understand that any breach of the above stated code will result in disciplinary action being taken.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

The academy exercise its right to monitor the use of the academy's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the academy's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Print name: …… Date: ……