

# Community First Academy Trust Social Media Policy



Community First  
Academy Trust

**ADOPTED AT THE MEETING OF DIRECTORS**

**28<sup>th</sup> March 2014**

**CHAIR OF BOARD: Mr J Pugh**

**This is a Trust-wide policy adopted and reviewed by either the Trust Board or Finance Committee and relates to all schools that are partners within the Trust.**

**Specific Academy policies, e.g. curriculum policies will be found on the individual school websites.**

**This policy was written in March 2017. It will be reviewed every three years by the Board of Trustees. Next review date: March 2020.**

## Contents

<b>1. Introduction .....</b>	<b>2</b>
<b>2. Purpose .....</b>	<b>2</b>
<b>3. Scope .....</b>	<b>3</b>
<b>4. Legal aspects .....</b>	<b>3</b>
<b>5. Official use of social media for the school .....</b>	<b>5</b>
<b>6. Personal use of social media .....</b>	<b>6</b>
<b>7. Online contact with children and young people .....</b>	<b>7</b>
<b>8. Online bullying and harassment .....</b>	<b>8</b>
<b>9. Summary .....</b>	<b>8</b>

## **1. Introduction**

Social Media is the term commonly given to websites and on-line tools which allow users to interact with each other by making new contacts and sharing information such as photographs, opinions, knowledge and interests.

There are different forms of social media which attract different audiences for different purposes and may include the \*following:

- Social networking sites such as Facebook, LinkedIn, Bebo and MYSpace
- Micro-blogging sites such as Twitter, Posterous and FriendFeed
- Video and image sharing sites such as YouTube, Flickr, Snapchat and Instagram

(\*not an exhaustive list)

## **2. Purpose**

The benefits of new technology and the new opportunities for communication which social media can bring are recognised, and it is also accepted that there are many uses for social media and some employees may wish to utilise such sites in a personal capacity.

The Academy may also encourage the use of IT Systems and Services for communicating with pupils, parents and the wider community for business related purposes therefore; this policy should be read in conjunction with the Academy's relevant IT Policies.

This policy is not intended to deter employees from enjoying social media but to highlight potential risks and to ensure that any content submitted on such sites does not compromise either their own reputation or that of the Trust, Academy, its pupils and employees.

It is also crucial that pupils, parents and the public have confidence in the Academies' decisions and services it provides and so this policy is designed to ensure all employees use social media responsibly so that confidentiality and reputation is safeguarded for the Trust, Academy, its pupils and all employees.

All employees are expected to comply with this policy, maintain suitable boundaries and conduct themselves in a manner that is appropriate and respectful. Failure to do so may result in action being taken as outlined in the Trust's Disciplinary Policy.

These expectations are also in line with Part 2 of the Teachers' Standards which relates to personal and professional conduct, and which all teachers are expected to observe and maintain.

If any breach of the policy involves a young person under eighteen years of age, an employee could be referred to the Disclosure and Barring Service and risk being barred from working with children and vulnerable adults in line with Keeping Children Safe in Education guidelines.

### **3. Scope**

This policy applies to all employees of the Trust including the Headteacher.

The principles of this policy also apply to any person who works on the Trusts premises including students on placement, agency, voluntary and casual workers, external consultants and contractors. Academies should ensure that people working on the premises are aware of the policy, for example as part of their introduction to the Academy, or within the contract for services.

The policy also applies whether sites are accessed via Academy equipment or not and whether or not they are accessed during working time and regardless of acting in an official or personal capacity.

It is for the Headteacher and Local Academy Board (LAB) of each Academy to decide whether they will allow staff to access social media whilst on Academy premises – for example during breaks/lunch-time for personal use, or in working time for research/professional purposes. The Academy must ensure that staff are aware of what is permitted, and staff must observe the provisions of this policy whenever they use social media.

The policy should be read in conjunction with the following policies, which include guidance on employees' responsibilities to ensure security of information by, for example, using passwords as appropriate, and logging out of sites once work is completed.

It is recognised that some Academies within the Trust may use social media as a legitimate means by which to communicate with pupils, parents and the community and in these circumstances, employees are authorised to use social media in line with paragraph 5 of this procedure.

### **4. Legal aspects**

Freedom of speech is a fundamental human right but it is a right that must be used responsibly. All employees should understand that they can be individually liable for any defamatory or untrue statements that they make on any social media sites whether they have identified themselves as an employee of the Academy or Trust or not. Furthermore, all employees must be aware that conduct online cannot always be isolated from their working life.

Employees should also be aware that if they chose to participate in any activity which compromises either their role within the Trust or the reputation of the Academy as a whole then this may leave the employee open to having legal action taken against them by either the Academy or a third party.

Currently the law states that if an action is illegal offline then it is also illegal online therefore, all employees need to be aware that Academy reserves the right to take disciplinary action against any employee who breaches any of the following:

## **4.1 Libel/defamation**

If an employee publishes either an untrue/defamatory statement or comment about another employee in work, or indeed about the Trust or Academy itself, which is deemed to be damaging to the reputation of either the individual or the Trust or Academy, then the individual or the Trust may choose to take legal action.

A successful libel claim will result in an award of damages against the employee.

The Acts that are likely to apply are:

- Libel Act 1843
- Defamation Acts 1952 & 1996
- Protection from Harassment Act 1997
- Criminal Justice & Public Order Act 1994
- Malicious Communications Act 1998

## **4.2 Copyright**

Any employee placing images or text from copyrighted sources (extracts from publications, photos etc.) without permission from Academy or otherwise is likely to breach the Copyright, Designs and Patents Act 1988. Employees should therefore not publish anything that they are either unsure about or which is deemed to be the property of Academy or Trust.

## **4.3 Disclosure of confidential information**

Confidential information may include person-identifiable information for example pupil and employee records, business records containing sensitive information and commercially sensitive information such as that relating to commercial proposals or current negotiations.

Employees should also not publish any personal data about other employees or pupils which includes photographs, videos etc.

The Acts that are likely to apply are:

- Data Protection Act 1998
- The Human Rights Act 1998
- Common Law Duty of Confidentiality

## **4.4 Obscene material**

Employees should never publish anything that is classed as obscene – this would be deemed to be a criminal offence. Obscene material is that which is designed to deprave or corrupt the audience. For the purpose of this policy 'obscene material' is that which will cause extreme offence to the Academy or Trust as a whole, its pupils or employees.

Publication of such material is considered a criminal offence and appropriate action will be taken.

#### **4.5 Offensive material**

Employees should never publish anything that is classed as offensive. 'Offensive', for the purpose of this policy, is material which is defamatory, racist or discriminatory on the grounds of religion, disability, gender or sexual orientation or alternatively which is designed, or is likely to, harass, victimise or bully, cause pain or distress to other employees, pupils or the Academy as a whole.

The Acts that are likely to apply are:

- Equality Act 2010
- Defamation Acts 1952 & 1996
- Protection from Harassment Act 1997
- Criminal Justice & Public Order Act 1994
- Malicious Communications Act 1998

#### **5. Official use of social media for the Academy or Trust**

Social media can be an appropriate and cost-effective way of making contact with residents, parents and the community, and some Academy's may choose to use such methods to assist in their communication processes.

Some employees may, therefore, be authorised by the Headteacher or Head of School to use social media in an official capacity. All employees must therefore read and understand this policy, before using social media, and must also set out clear parameters and the purpose for which they are permitted to use it in an official capacity on behalf of the Trust/Academy.

Employees using social media in an official capacity should always disclose who they are and who they represent. They must not engage in conduct which would not be acceptable in the workplace, and must act in accordance with the provisions of this policy, and be aware of the legal aspects as outlined above.

#### **6. Personal use of social media**

All employees have a personal responsibility for their own online behaviour and activities and must ensure their use of any social media sites takes place within appropriate professional boundaries.

As a guide, the following should be adhered to by all employees:

- Employees should be cautious about identifying themselves as employees of the Trust or Academy. This is to prevent information from being linked with the Academy or the Trust and to safeguard the privacy of other employees. However, in certain circumstances, it may be acceptable, for example whilst using 'professional forums', which by their very nature relate to job role/profession eg LinkedIn.

- The Academy does not expect employees to discontinue contact with their family members via any social media sites if the Academy starts to provide a service for them (for example if their child becomes a pupil of the Academy) however, any information employees obtain in the course of their employment with Academy must not be used for personal gain nor be passed on to others who may use it in such a way.
- Employees should not have any contact with pupils' family members (unless they are related) through social media sites if that contact is likely to compromise their professional position or constitute a conflict of interest or call into question their objectivity.
- Information which employees have access to as part of their employment which may include personal information about pupils and their family, colleagues and information about the Academy or Trust must not under any circumstances be discussed in any way on any social media sites. The only exception to this may be where social media is being used for official Academy or Trust purposes, as outlined in paragraph 5 above.
- Photographs, videos or any other types of images of pupils, their families or images depicting Academy employees wearing their uniforms (if applicable) or anything which contains the Academy or Trust logo must not be published on any social media sites.
- Academy email addresses and other Academy contact details must not be used by employees for the purpose of setting up personal social media accounts or to communicate through such sites.
- Employees are advised to be cautious if they choose to invite work colleagues to be 'friends' on personal social media sites as this may blur the line between work and personal lives and it may be difficult to maintain a professional working relationship if for example too much 'personal' information is known.
- Employees are advised to ensure their 'privacy settings' are set at the appropriate level on any social media sites and to opt out of public listings in order to protect their own privacy.
- Employees should consider doing a Google search on their own name to check what information is held online about them. If any content is found that they would prefer not be accessible, they can request that this is removed, by asking the person who uploaded it if the person is known by them, or if appropriate, by using the "report abuse" facility within the particular site.
- Employees are advised to keep their log-in details and passwords confidential at all times in order to ensure no other person can access their accounts.

## **7. Online contact with children and young people**

There is a concern that social media sites may increase the potential for sexual exploitation of children and young people or provide the opportunity for 'grooming' to take place. It is also possible that employees who work with children may be at risk of false allegations being made against them.

It is therefore vital that employees who use social media take appropriate steps to protect themselves from such allegations, maintain appropriate boundaries, exercise their professional judgement and avoid any contact that may lead to their intent and motivations being questioned.

As a guide, the following should be adhered to by all employees:

- Employees should not share personal information with pupils
- Employees must not have contact through any social media sites with any pupil whether from their current Academy establishment or another unless that pupil is a family member.
- Should a pupil attempt to contact an employee via any social media sites then this should be reported to the Headteacher immediately.
- Employees must decline all 'friend requests' they receive from any pupil or young person to whom they have acted in a position of trust whether in their current Academy establishment or another.
- Employees who leave employment from their current Academy must not contact pupils by means of social media sites if this compromises their professionalism or objectivity.
- Employees should be cautious when using such sites at Twitter or other online chat rooms as it may be difficult to ascertain to whom they may be chatting.

## **8. Online bullying and harassment**

Social media can have potential dangers and drawbacks as both adults and children have found themselves the target of online abuse, harassment and bullying which is often referred to as 'cyber bullying' which includes:

- Name calling
- Malicious comments
- Exclusion
- Intimidation
- Spreading of rumours
- Bombarding with unwanted messages

Cyber bullying can have a significant impact on health and wellbeing and will not be tolerated. Should any employee feel they have been a victim of cyber bullying this should be reported to the Headteacher in the first instance. If it is the Headteacher who is the victim of concern should be raised with the CEO or Chair of the LAB.

## **9. Summary**

All employees have a personal responsibility for their online behaviour and ensuring their use of social media falls within appropriate professional boundaries.

Any inappropriate use of social media by employees which breaches this policy may be treated as misconduct under the Trusts Disciplinary Procedure for and could potentially constitute gross misconduct which could result in employment being terminated. If this involves a young person under eighteen years of age, an employee could be referred to the Disclosure and Barring Service and risk being barred from working with children and vulnerable adults.

Employees who choose to use social media should therefore:

- Consider how their online presence could possibly compromise their professional responsibilities.
- Think carefully before posting information, photographs or comments on the Internet.
- (Things they might have thought funny at the time could potentially cause embarrassment to them or others and, online records are easy to create, but can be difficult, or in some cases, impossible to remove).
- Exercise caution when divulging personal information online, for example date of birth, home address etc, as this could potentially put them at risk of identity theft.
- Not give out personal contact details to pupils – mobile number, email address etc.
- Consider doing a Google search on their own name to check what information is held online about them. If any content is found that they would prefer not be accessible, they can request that this is removed, by asking the person who uploaded it if the person is known by them, or if appropriate, by using the “report abuse” facility within the particular site.
- Ensure they protect their social media profile by utilising privacy settings so only friends are able to access and comment on their pages.
- Be aware that their information could still appear on friend’s pages, which may be publicly accessible.
- Be aware that friends can ‘tag’ them into photographs which they may not wish to be Never request/ accept ‘personal’ Facebook friend requests, or communicate online with pupils, ex-pupils who are under the age of eighteen, or parents if that contact is likely to compromise the employee’s professional position or constitute a conflict of interest or call into question their objectivity.
- Check who is “following” them on Twitter and block pupils, ex-pupils and parents from receiving their updates.
- Refrain from identifying their place of work, or making reference to the Academy on social media sites. Publicly available – employees should therefore ask people not to tag them into photographs etc without their consent. Employees can also ‘un-tag’ themselves from Facebook photographs.
- Maintain an appropriate distinction between professional and personal life. Employees who have an additional relationship with the Academy, for example if their own children are pupils, or if they are active members of the community should not use online forums to raise any grievances they may have in relation to Academy.
- Ensure that they have a strong password for all social media sites and that electronic security is maintained by password protecting equipment, never sharing passwords and logging out fully after use. This will include ensuring that Academy and personal property including mobile phones, laptops, I-Pads etc are kept secure, so that children are not able to access them.
- Never make, respond, or take part in an online conversation that includes any offensive, abusive, derogatory, defamatory or inappropriate comments related to colleagues, pupils, parents or the Academy on any social media sites and be conscious that information they disclose and opinions that are expressed

are in the public domain and as such, could potentially bring them and/or the Academy into disrepute.

- Ensure that their own personal views cannot be misconstrued as them speaking on behalf of the Academy or Trust. (an employee is advised to use statements such as, “my view is..” or “in my opinion..” )
- Always comply with Academy’s policies/ guidance on use of technology.
- Never divulge any confidential information relating to Academy.
- Not use social networking sites for personal use during working hours.
- Not post any photographs or video footage taken at Academy onto websites without obtaining express written permission to do so.
- In the event that an employee feels they have been a target of cyber bullying or inappropriate online behaviour, keep the evidence (screen prints, emails etc) and report what has happened to the Headteacher or Head of School, or a member of the Leadership team. However, extreme caution must be exercised in relation to obscene material and staff members should not retain copies of information, but should instead report their concerns immediately to the Headteacher for further investigation.
- Be mindful of their professional responsibilities when using social media and be conscious that managing their online reputation is important for their current and future career. (There is an increasing trend for employers to access social networking sites before interviewing job applicants so there is potential that their online activities could prevent them from progressing in their career). Equally, an employee could face disciplinary action if their employer feels that their use of social networking is inappropriate.