



# Social Media Policy

<b>Status</b>	<b>Statutory</b>
<b>Responsible Directors</b>	<b>Education and Standards Committee</b>
<b>LGB</b>	<b>Full Local Governing Board</b>
<b>Responsible Persons</b>	<b>CEO</b>
<b>Date Policy Agreed</b>	<b>Sept 2017</b>
<b>Review Date</b>	<b>Sept 2022</b>
<b>Date of next review</b>	<b>September 2023</b>



## Contents

Introduction.....	3
Purpose.....	3
Safeguarding.....	4
Roles and Responsibilities.....	4
Legal Framework.....	5
Definition of Social Media.....	6
Use of Social Media.....	6
Employee Responsibility.....	7
Personal use of Social Media – Employee Responsibility.....	8
Using Social Media on behalf of the Trust.....	9
Disciplinary Action.....	9
Social Media Security.....	10
Monitoring the Use of Social Media Websites.....	10
Employee Groups / Networks.....	10

### Version Control

Version	Revision Date	Revised by	Section Revised
V1	New Policy		
V2	August 2021	L Burton	Throughout Executive Principal replaced with CEO Local Governing Body replaced with Local Governing Board Page 5 updated to latest Data Protection Act 2018
V3	September 2022	L Burton	No changes

## Introduction

This policy applies to all teaching and other staff employed by The Exceed Learning Partnership Trust, trainee teachers, other trainees, volunteers and other individuals who work for or provide services on behalf of the academies within the trust, (within this policy referenced as employee(s) or academy staff)

The policy also applies to members of Local Governing Boards and all Members on the Board of the Academy Trust as follows:

- Whilst some aspects of this policy are clearly more targeted at employees, many have equal application to governors and members of the Trust Board. For example, the policy provides guidance for all on what is considered to be inappropriate use of social media / internet sites. All Governors and members of the Trust Board should therefore ensure that they comply with the spirit of this policy;
- Though Governors or Trust Board Members would not be subject to the same disciplinary process as staff, there are still forms of redress available should a governor/trust board member behave in an inappropriate manner. The appropriate procedures would be followed in such cases

## Purpose

The primary purpose of this policy is to clarify how employees should conduct themselves when using all forms of social networking websites and blogs, whether conducted through their Academy's media, personal media and in work time or in one's own time.

Employees wanting to create a work-related social media site must discuss this with, and obtain the relevant approval from, the Principal/CEO

If followed, this policy will guide employees on how to minimise the risk they may place themselves and pupils in when they choose to write about their work or matters relating to the Academy, the Trust and their personal lives. This in turn will minimise situations where safeguarding concerns could arise, employee's integrity or professional standing could be undermined, or the Academy or the Trust brought into disrepute and professional relationships with colleagues and pupils compromised.

Additionally, adhering to this policy reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of any breaches of confidentiality, privacy, libel, defamation, harassment and copyright laws.

This policy is not intended to prevent employees from using social media sites, but to make them aware of the risks they could face when sharing information about their professional and/or personal life.

This policy covers content that is published on the internet (e.g. contributions in blogs, message boards, social networking sites or content sharing site and applications – ‘apps’) even if created, updated, modified, shared and contributed to outside of working hours or when using personal IT systems. The internet is a fast-moving technology and it is impossible to cover all circumstances of emerging media - the principles in this policy must be followed irrespective of the medium.

## **Safeguarding**

We have a duty of care to ensure that all our pupils are safe.

This policy is adopted in line with the Trusts’ policies for Safeguarding and E Safety and the expectations and procedures related to them.

Employees and Members of the Trust should at all times consider the safety and wellbeing of our pupils when embarking on social media activities

## **Roles and Responsibilities**

Exceed Learning Partnership Trust will

- Review this policy every year and/or in response to any significant changes to social media issues; medium or external factors

The Local Governing Board will:

- Ensure the principles of the Social Media Policy are embedded and evident in the academy.

The Principal/CEO will

- Have overall responsibility for social media sites and publications within them in their academy. The day-to-day management of this can be delegated to a staff member.
- Delegate the responsibility for the technical elements of social media to a member of support staff.
- Ensure staff understand the expectations of social media use outlined in this policy, with particular attention to ensure the safeguarding of pupils and staff

ICT support will:

- Inform the Principal/CEO and the E-safety officer of requests for new social media sites.
- Ensure filtering and monitoring solutions are fit for purpose and limit access to social media sites where appropriate and monitor internet/email use.
- Inform the Designated Safeguarding Lead or Senior Leader responsible (depending on the event) of any event that may concern them.

Parents and Carers will be encouraged to:

- Understand and accept the academy /trust need to follow these principles to ensure the professional use of digital media and social sites and the safeguarding of pupils and staff.

## **Legal Framework**

Exceed Learning Partnership is committed to ensuring that all staff members provide confidential services that meet the highest standards. All staff members are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work.

(refer to Data Protection Policy)

Confidential information includes, but is not limited to:

- Person-identifiable information e.g. pupil and employee records protected by the Data Protection Act 2018
- Information divulged in the expectation of confidentiality
- Academy business or corporate records containing organisation or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information

Exceed Learning Partnership and its academies could be held vicariously responsible for acts of their employees. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work, may render the Trust and the Academy liable to the injured party.

Social media should never be used in a way that breaches any Trust/Academy policy.

It should be noted that individuals can be identified as working for the Academy/Trust simply by revealing their name or a visual image of themselves.

## Definition of Social Media

Social media can be defined as websites and applications that enable users to create and share content or to participate in social networking, resulting in a number of different activities. These activities can include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter or LinkedIn;
- Writing or commenting on a blog, whether it is your own or the blog of another person/information site;
- Taking part in discussions on web forums or message boards;
- Leaving product or service reviews on business websites or customer review websites;
- Taking part in online polls;
- Uploading multi-media on networking sites such as Instagram and Tumblr;
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account.

## Use of Social Media

As with all personal internet use, employees using social media sites must observe the specific requirements of their Academy's E-safety Policy.

Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against employees and the Academy/Trust. It may also cause embarrassment to the Academy and other parties connected to the Academy, or bring such parties into disrepute. Any such action would likely be addressed under the Disciplinary Policy and could result in summary dismissal.

Where evidence of misuse is found, a more detailed investigation in accordance with the Disciplinary Policy may be necessary, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police.

Any employee who becomes aware of any use of social media by other member of staff which is in breach of this policy should report the matter to the Principal/CEO



## Employee Responsibility

When using any form of social media, whether for work or personal use, employees must ensure that they behave responsibly, taking account of the following requirements:

- Employees must be conscious at all times of the need to keep personal and professional lives separate. Employees should not put themselves in a position where there is a conflict between work for the Academy and personal interests.
- Employees are personally responsible for the content they publish on social media sites, including likes, re-tweets, etc. Employees should assume that everything that is written is permanent and can be viewed by anyone at any time.
- Employees should assume that everything can be traced back to them personally, as well as to their colleagues, Academy and parents.
- To avoid any conflict of interest, employees should ensure that personal social networking sites are set at private and pupils are never listed as approved contacts. An exception to this may be if the child is the employee's own child or relative.
- Information must not be posted that would disclose the identity of pupils.
- Employees must ensure content or links to other content does not interfere with their work commitments.
- Pupils must not be discussed on social media sites.
- Employees should not post information on sites (including photographs and videos) that could bring the Academy or the Trust into disrepute.
- Potentially false or defamatory remarks towards the Academy, the Trust, employees, pupils, pupils' relatives, suppliers and partner organisations should not be posted on social media sites.
- Employees must not either endorse or criticise service providers used by the Academy, the Academy or the Trust or develop on-line relationships which create a conflict of interest.
- When posting on social media sites employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, discriminatory language which may cause embarrassment to the Academy, the Trust, employees, pupils, pupils' relatives, suppliers and partner organisations.
- Employees must not divulge any information that is confidential to the Academy, the Trust or a partner organisation.
- Employees must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
- Employees must not upload, post, forward or post a link with regards to any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or material in breach of copyright or other intellectual property rights, or which invades the privacy of any person.
- Employees must not represent their personal views as those of the academy or the trust, on any social medium. Any expressions, idea or opinions that are made a

disclaimer such as ‘these are my own personal views and not those of the academy’ should be added.

(This list is not exhaustive).

### **Personal use of Social Media – Employee Responsibility**

- Staff members must not have contact through any form of personal social media site with any pupil, whether from your Academy or any other Academy, unless the pupils are family members.
- Staff members must not have any contact with pupils’ family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the Academy/Trust (where applicable)
- Staff members must decline ‘friend requests’ from pupils they receive in their personal media accounts. If any such requests from pupils, who are not family members, are received they must discuss this with the Academy/Trust designated safeguarding lead.
- On leaving the Academy/Trust service, staff members must not contact academy/trust pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal media sites.
- Information staff members have access to as part of their employment of the Academy/Trust, including personal information about pupils and their family members, colleagues, and other parties and Academy corporate information must not be discussed on their personal web space.
- Photographs, videos or any other types of digital images depicting pupils wearing uniforms or clothing with Academy logos or images identifying Academy premises must not be published on staff personal web space
- Academy/Trust addresses and other official contact detail must not be used for setting up personal social media accounts or to communicate through such media.
- Staff members must not edit open access online encyclopedias such as Wikipedia, in a personal capacity at work. This is because the source of the correction will be recorded as the Academy’s/Trust’s IP address and the intervention will, therefore, appear as if it comes from the employer.



- Academy, Trust logos or brands must not be published on personal web space.
- Staff members should not provide references for other individuals on social or professional networking sites (such as LinkedIn), as such references, positive or negative, can be attributed to the academy/Trust and create legal liability for both themselves and the academy/Trust
- Staff members must use appropriate security settings on social media sites in order to mitigate any potential issues. Staff members are advised to set their privacy levels of their personal web sites as strictly private as they can and to opt out of public listings on social networking sites to protect their own privacy.
- Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use separate email addresses just for social networking so that any other contact details are not given away.

### **Using Social Media on behalf of the Trust**

A list will be kept of any permitted sites that are used within the Academy/Trust.

Staff members can only use permitted sites for communicating with pupils or to enable pupils to communicate with one another.

There must be strong pedagogical or business reasons for creating official Academy/Trust sites to communicate with pupils and others. Staff must not create sites for trivial reasons which could expose the Academy to unwelcome publicity or cause reputational damage.

The Academy is expected to hold a Twitter account on their website and to keep it up to date.

Official Academy sites and social media profiles must be created only according to the requirements as outlined within this policy.

### **Disciplinary Action**

Employees should be aware that the use of social media sites in a manner contrary to this policy, including if others implicate you in a breach of any of the terms listed above, may result in disciplinary action and in serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

Any instances of “cyber bullying” will initially be addressed under the Dignity at Work Policy and Procedure and may result in disciplinary action.

## Social Media Security

Employees should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for false allegations and threats. In addition, it may be possible, through social media sites, for children or vulnerable adults to be identified, which could have implications for their security.

Furthermore, there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to their professional reputation and that of the Academy/Trust. In addition, it may be possible for other social media site users to identify where employees live, which could have implications for individual security.

Therefore, first and foremost consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above.

## Monitoring the Use of Social Media Websites

Employees should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this policy are found, action may be taken under the Disciplinary Policy.

The Academy Trust considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

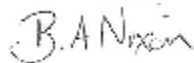
- Been using social media websites when he/she should be working; or
- Acted in a way that is in breach of the rules set out in this policy.

## Employee Groups / Networks

Employee groups can be created on social media sites such as Facebook. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate and not in breach of any of the terms in this policy.

Policy Agreed: 13<sup>th</sup> September 2017 and reviewed September 2022

Signed Executive Principal:



Signed: Chair of Directors:



Policy to be reviewed: Autumn 2023