u

Social Media Policy

Date of Policy	2025
Reviewed and Agreed by	The Directors' Board
Review Date	Autumn 2025
Next Review Date	Autumn 2026

Social Media Policy

Contents:

Statement of intent, Definitions, Scope, Principles, Expectations

Appendices

Do not use social networking sites or online blogs to make comments on anything related to The Societas Trust, its academies, its activities, its pupils, parents, partners, governors or colleagues.

Statement of intent and Definitions

The Societas Trust ("The Trust") understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our pupils against potential dangers when accessing the internet at school, and to educate our pupils about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and pupils in support of the school's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyberbullying and potentially career damaging behaviour.
- Arranging online safety meetings for parents.

We also recognise that Social media enables organisations to build connections and relationships, share positive news and information quickly and respond to queries swiftly. Social media can also provide valuable channels that are useful for communicating during an emergency or crisis when information needs to be shared rapidly. This policy provides guidance on how to maximise the benefits of social media, minimise the risks and ensure consistent high standards of social media use.

Definitions

Social media is the term commonly given to internet and mobile-based channels and tools that allow users to interact with one another and share opinions and content. As the name implies, social media involves the building of communities or networks that encourage participation and engagement.

Social media allows parties to communicate instantly or to share data in a public forum via websites or apps. This includes, but is not limited to, online forums, blogs, video and image sharing websites and social platforms such as YouTube, Facebook, X (formerly known as Twitter), Instagram, SnapChat, TikTok, SlideShare and LinkedIn as well as messaging apps such as WhatsApp and Facebook Messenger.

The nature of social media is such that it is rapidly evolving and we appreciate that there may be communication platforms which emerge in the future, but which are not currently in existence.

Scope

The policy applies to all Trust employees, governors, agency workers, volunteers or those engaged in consultancy work.

Principles

The Trust's Information Security Policy makes it clear what is acceptable internet use when employees are at work; access to most networking sites is restricted so access is prevented during work time. All employees must be fully informed of this policy and what is deemed to be acceptable usage of Trust / Academy equipment and internet services.

It is advisable that all employees demonstrate online awareness and take precautions to avoid leaving themselves vulnerable to allegations relating to the posting of comments and other material online. (Appendix E)

This policy may be used in conjunction with other Trust / Academy policies to address online abuse such as inappropriate activities, obscenity, harassment and any form of discrimination or unwanted behaviour towards colleagues; pupils, their families and other members of the community.

The Trust's Code of Conduct, Confidential Reporting, Information Security, Data Protection and Equal Opportunities policies may also set out guidance for online activity (this list is not exhaustive).

The policy has been consulted upon with recognised Teaching and Support Staff Trade Unions.

Expectations

The pupils, parents, carers, colleagues and governors are entitled to expect the highest standards of conduct and professionalism from all those who work for the Trust, including participation on social networking sites.

Anyone subject to threats, abuse or harassment via their use of social networking sites whilst working on behalf of the Trust should report the incidents to their Head Teacher / Manager immediately.

Anyone working on behalf of the Trust who is subjected to threats, abuse or harassment via social networking sites from a colleague, pupil, member of the pupil's family or other relevant person, should report the incidents to the Head Teacher / Manager immediately.

1 Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- DfE (2023) 'Data protection in schools'
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010
- DfE (2025) 'Keeping children safe in education 2025'
- Guidance for Safer Working Practice for Adults who work with Children and Young People' September 2019 (Staffordshire and Stoke on Trent Safeguarding Children Boards)

This policy operates in conjunction with the following Trust/ school policies (List is not exhaustive):

- Code of Conduct for Parents and Carers
- Device and Technology Acceptable Use Agreement for Staff
- Device and Technology Acceptable Use Agreement for Pupils
- Online Safety Policy
- Data Protection Policy
- Behaviour Management Policy
- Complaints Policy
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Low-level Safeguarding Concerns Policy
- Mobile Phone and Camera Policy
- Code of Conduct
- Confidential Reporting Policy
- Cyber-Crime Response Plan
- Safeguarding and Child Protection Policy
- Professional Boundaries with Pupils Policy
- Disciplinary Policy and Procedure
- Behaviour Policy
- School Social Media Accounts – Terms of Use Agreement

2 Roles and responsibilities

The governing board will be responsible for:

- Ensuring this policy is implemented by the setting.
- Reviewing this policy on an annual basis.
- Ensuring the DSL's remit covers online safety.

- Ensuring their own knowledge of social media and online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that this policy, as written, does not discriminate on any grounds, including against any of the protected characteristics, as outlined in the Equality Act 2010.

The headteacher will be responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and pupils are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- In conjunction with the governing board, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside the DPO and IT technicians to ensure appropriate security measures are implemented and compliance with UK GDPR and other data protection legislation.

The DSL will be responsible for:

- The school's approach to online safety.
- Dealing with concerns about social media use that are safeguarding concerns.

Staff members will be responsible for:

- Adhering to the principles outlined in this policy and the Device and Technology Acceptable Use Agreement for Staff.
- Ensuring pupils adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff, pupils or parents to the headteacher immediately.
- Attending any training on social media use offered by the school.

Parents will be responsible for:

- Adhering to the principles outlined in this policy and the Social Media Code of Conduct for Parents.
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.
- Attending meetings held by the school regarding social media use wherever possible.

Pupils will be responsible for:

- Adhering to the principles outlined in this policy and the Pupil Code of Conduct.
- Ensuring they understand how to use social media appropriately and stay safe online.
- Seeking help from school staff if they are concerned about something they or a peer have experienced on social media.
- Reporting incidents and concerns relating to social media in line with the procedures within this policy.
- Demonstrating the same high standards of behaviour as expected within the school.

The Academy Business Manager will be responsible for:

- Monitoring and reviewing all setting-run social media accounts.
- Vetting and approving individuals who wish to be 'friends' or 'followers' on the school's social media platforms.
- Consulting with staff on the purpose of the social media account and the content published.
- Maintaining a log of inappropriate comments or abuse relating to the school.
- Handling inappropriate comments or abuse posted on the school's social media accounts, or regarding the school.
- Creating a terms of use agreement, which all content published must be in accordance with.
- Ensuring that enough resources are provided to keep the content of the social media accounts up-to-date and relevant.

IT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's social media accounts.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

3 Setting Social Media Accounts

Social media accounts for the setting will only be created by the School/ Academy Business Manager and other designated staff members, following approval from the headteacher. A school-based social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official school email account.

When setting up a school social media account, consideration will be given to the following:

- The purpose of the account
- Whether the overall investment will achieve the aim of the account
- The level of interactive engagement with the site
- Whether pupils, staff, parents or members of the public will be able to contribute content to the account
- How much time and effort staff members are willing to commit to the account
- How the success of the account will be evaluated

The headteacher will be responsible for authorising members of staff and any other individual to have admin access to school social media accounts. Only people authorised by the headteacher will be allowed to post on the school's accounts.

Passwords for the setting's social media accounts are stored securely on the school's IT network. The passwords are only shared with people authorised by the headteacher.

All posts made to school social media accounts will not breach copyright, data protection or freedom of information legislation.

The setting's social media accounts will comply with the platform's rules. The marketing officer will ensure anyone with authorisation to post on the school's social media accounts are provided with training on the platform and the rules around what can be posted.

The setting's social media accounts will be moderated by the Academy Business Manager or another designated member of staff.

Staff conduct

Only staff with authorisation from the headteacher will post on school accounts and they will adhere to the School Social Media Accounts – Terms of Use Agreement.

Staff will get content approved by the Academy Business Manager before it is posted. Staff will only post content that meets the school's social media objectives, including the following:

- Reminders about upcoming events
- Good news regarding the school's performance, attainment or reputation
- Good news regarding the achievements of staff and pupils
- Information that parents should be aware of, e.g. school closure

Staff will ensure that their posts meet the following criteria:

- The post does not risk bringing the school into disrepute
- The post only expresses neutral opinions and does not include any personal views
- The post uses appropriate and school-friendly language
- The post is sensitive towards those who will read it, and uses particularly neutral and sensitive language when discussing something that may be controversial to some
- The post does not contain any wording or content that could be construed as offensive
- The post does not take a side in any political debate or express political opinions
- The post does not contain any illegal or unlawful content

4 Staff use of personal social media

Staff will not be prohibited from having personal social media accounts; however, it is important that staff protect their professional reputation by ensuring they use personal social media accounts in an appropriate manner.

Staff will be required to adhere to the following guidelines when using personal social media accounts:

- Staff members will not access personal social media platforms during school hours.
- Staff members will not use any school-owned mobile devices to access personal accounts.
- Staff will not 'friend', 'follow' or otherwise contact pupils through their personal social media accounts. If pupils attempt to 'friend' or 'follow' a staff member, they will report this to the headteacher.
- Staff will be strongly advised to not 'friend' or 'follow' parents on their personal accounts.
- Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee of the school on their personal social media accounts.
- Staff will ensure it is clear that views posted on personal accounts are personal and are not those of the school.
- Staff will not post any content online that is damaging to the school, its staff or pupils.
- Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Staff will not post comments about the school, pupils, parents, staff or other members of the school community.

Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal. Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.

Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

5 Parent social media use

Parents are able to comment on or respond to information shared via social media sites; however, parents should do so in a way which does not damage the reputation of the school.

Parents will be asked not to share any photos or personal details of pupils when commenting on school social media sites, nor post comments concerning other pupils or staff members, in accordance with the Social Media Code of Conduct for Parents.

Any parents that are seen to be breaching the guidance in this policy will be required to attend a meeting with the headteacher, and may have their ability to interact with the social media websites removed.

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution.

6 Pupil social media use

Pupils will not access social media during lesson time, unless it is part of a curriculum activity. Pupils will not be permitted to use the school's WiFi network to access any social

media platforms unless prior permission has been sought from the headteacher, and an IT technician has ensured appropriate network security measures are applied.

Pupils will not attempt to 'friend', 'follow' or otherwise contact members of staff through their personal social media accounts. Where a pupil attempts to 'friend' or 'follow' a staff member on their personal account, it will be reported to the headteacher.

Pupils will not post any content online which is damaging to the school or any of its staff or pupils. Pupils will not post anonymously or under an alias to evade the guidance given in this policy.

Pupils are instructed not to sign up to any social media platforms that have an age restriction above the pupil's age.

If inappropriate content is accessed online on school premises, this will be reported to a member of staff.

Breaches of this policy will be taken seriously, and managed in line with the Behaviour Policy.

7 Data protection principles

The school will obtain consent from parents at the beginning of each academic year using the Social media consent form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the entire academic year. Consent provided for the use of images and videos only applies to school accounts – staff, pupils and parents are not permitted to post any imagery or videos on personal accounts.

A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The DPO will be responsible for ensuring this consent record remains up-to-date.

Parents are able to withdraw or amend their consent at any time. To do so, parents must inform the school in writing. Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and pupils' requirements following this. Wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.

Consent can be provided for certain principles only, for example only images of a pupil are permitted to be posted, and not videos. This will be made explicitly clear on the consent from provided. The school will only post images and videos of pupils for whom consent has been received.

Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the Academy Business Manager for use. Only appropriate images and videos of pupils will be posted in which they are suitably dressed, e.g. it would not be suitable to display an image of a pupil in swimwear.

When posting on social media, the school will use group or class images or videos with general labels, e.g. ‘sports day’.

When posting images and videos of pupils, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified. The school will not post pupils’ personal details on social media platforms and pupils’ full names will never be used alongside any videos or images in which they are present.

Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

Any breaches of the data protection principles will be handled in accordance with the school’s Cyber-security Policy.

8 Safeguarding

Any disclosures made by pupils to staff about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Concerns regarding a staff member’s online behaviour will be reported to the headteacher, who will decide on the best course of action in line with the relevant policies, e.g. the Code of Conduct and Disciplinary Policy and Procedures. If the concern is about the headteacher, it will be reported to the CEO. If the concern is about the CEO, it will be reported to the Chair of the Trust.

Concerns regarding a pupil’s online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the headteacher and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the headteacher will contact the police. The school will avoid unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

As part of the usual communication with parents, the school will reinforce the importance of pupils being safe online and inform parents what systems the school uses to filter and monitor online use. The school will also make it clear to parents what their children are being asked to do online for school. including what platforms they will be asked to access and who from the school, if anyone, they will be interacting with online.

9 Blocked content

In accordance with the school's Cyber-security Policy, the online safety officer will install firewalls on the school's network to prevent access to certain websites. The following social media websites are not accessible on the school's network:

- X
- Facebook
- Instagram

IT technicians retain the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.

Inappropriate content accessed on the school's computers will be reported to an IT technician so that the site can be blocked. Requests may be made to access erroneously blocked content by submitting a blocked content access form to an IT technician, which will be approved by the headteacher.

10 Cyberbullying

Any reports of cyberbullying on social media platforms by pupils will be handled in accordance with the Anti-bullying Policy.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy. Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.

11 Training

The school recognises that early intervention can protect pupils who may be at risk of cyberbullying or negative social media behaviour. As such, staff will receive training in identifying potentially at-risk pupils. Staff will receive training on social media as part of their new starter induction. Staff will receive regular and ongoing training as part of their development.

Pupils will be educated about online safety and appropriate social media use on a termly basis through a variety of mediums, including assemblies, PSHE lessons and cross-curricular links. Pupils will be provided with material to reinforce their knowledge.

Parents will be invited to online safety and social media training on an annual basis and provided with relevant resources, such as our Social Media Code of Conduct for Parents.

Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

12 Monitoring and review

This policy will be reviewed on an annual basis by the Directors Board.

Appendix A

Blocked content access request form

Requester	
Staff name	
Date	
Full URL	
Site content	
Reasons for access	
Identified risks and control measures	
Authoriser	
Approved?	
Reasons	
Staff name	
Date	
Signature	

Appendix B

Inappropriate content report form

Staff name (submitting report)	
Name of individual accessing inappropriate content (if known)	
Date	
Full URL(s)	
Nature of inappropriate content	
To be completed by IT technician	
Action taken	
Staff name	
Date	
Signature	

Appendix C

Social media site creation approval form

Use of social media on behalf of the school must be approved by the headteacher prior to setting up sites. Please complete this form and return it to the headteacher.

Team details		
Department		
Moderator of site		
Purpose of using social media		
Please describe why you want to set up this site and the content of the site		
What are your aims and what do you hope to achieve by setting up this site?		
What is the proposed content of the site?		
Proposed audience of the site		
☐ Pupils of the school Ages: **age range**	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: **name of school**	☐ Members of the public
☐ Other (please give details)		
Proposed contributors to the site		
☐ Pupils of the school Ages: **age range**	☐ School staff	☐ Pupils' family members
☐ External organisations	☐ Pupils from other schools Schools involved: **name of school**	☐ Members of the public

☐ Other (please give details)	
Administration of the site	
Names of administrators (the site must have at least **two** approved administrators)	
Who will vet external contributors? (Please state name and job role)	
Who will host the site?	
Proposed date of going live	
How do you propose to advertise for contributors?	
If contributors include pupils, how do you propose to inform and obtain the consent of parents or responsible adults?	
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' and 'followers' etc. of the site?	
Approval	
Approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher.	

Marketing officer **I approve the aims and content of the proposed site and the use of the school brand and logo.**	**Name**	
	Signature	
	Date	

Headteacher **I approve the aims and content of the proposed site and the use of the school brand and logo.**	**Name**	
	Signature	
	Date	

Appendix D

Social media consent form

This consent form provides information pertaining to how **name of school** wishes to use personal data on social media, details the terms under which the school will use this data and requests consent for the school to use your personal data on social media.

Name of parent	
Name of pupil	
Year group	

Why do we need your consent?

The school requests the consent of parents on an **annual** basis to use images and videos of their child for a variety of different purposes.

Without your consent, the school will not use images, videos, names or other forms of personal data of your child on social media. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why will we be using personal data on social media?

The school wants to use certain types of data on social media to promote the positive and inclusive ethos of the school – we aim to celebrate our pupils' and school's achievements and social media allows us to do this.

Where the school uses images of individual pupils, the name of the pupil **will not** be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil **will not** be used to accompany the text.

If, for example, a pupil has won an award and their parent would like their name to be published alongside their image, **separate consent** will be obtained prior to this.

With your consent, the school may use personal data on social media, the school website, in school prospectuses and other printed publications, such as a newsletter.

Who will be able to see the data once it's on social media?

The school's privacy settings only allow people who have been accepted to view the content on our social media platforms; additionally, where it is possible, the school's settings do not allow for further sharing. Please note, this sharing restriction may not be possible on all social media platforms, meaning that, if the content has been posted and is subsequently shared, more people will be able to view that piece of content.

What are the conditions of use?

- This consent form is valid for **the current academic year**.

- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video on social media.
- The school will not include personal emails, postal addresses, or telephone or fax numbers on images or videos on social media.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may post pictures of work created by pupils on social media.
- The school may use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- The school will not post any sensitive data, such as details of SEND, without express and additional consent, and will then still anonymise the posts.

Providing your consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

The school will **only** post personal data on social media for the conditions that you provide consent for.

I provide consent to	**Yes**	**No**
Using images of my child on the school's social media accounts.		
Using videos of my child on the school's social media accounts.		
Using images of my child on social media, including the following: **[Delete and/or add as appropriate]** • **X** • **Facebook** • **Instagram**		
Using videos of my child on social media, including the following: **[Delete and/or add as appropriate]** • **X** • **Facebook** • **Instagram**		
Using my child's first name on social media.		
Using my child's age on social media.		

Refreshing your consent

This form is valid for **the entire academic year**, it will be updated on an **annual** basis. Parents are required to fill in a new form for their child **every academic year**.

Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share pupil images and videos
- Changes to a pupil's circumstances, e.g. safeguarding requirements mean a pupil's image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing to the data protection officer (DPO). A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent

Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing personal data that was shared prior to withdrawal; however, the school will make every effort to remove posts about the pupil where possible, e.g. images of the pupil on social media will be removed.

If you would like to withdraw your consent, you must submit your request in writing to the DPO.

Declaration

I, _____ (name of parent), understand:

- Why my consent is required.
- The reasons why **name of school** uses my child my child's personal data on social media.
- Who will be able to view my child's personal data once posted.
- The conditions under which the school uses personal data of my child on social media.
- I have provided my consent above as appropriate, and the school will act in accordance with my requirements.
- Consent is refreshed on an **annual** basis and I must re-provide consent in subsequent academic years.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the DPO.

Name of parent: _____

Signature: _____

Date: _____

If you have any questions regarding this form, please do not hesitate to contact the DPO at **email address** or **phone number**.

Appendix E

Online awareness

Employees are reminded of the following points:

1) They are legally liable for anything posted online.

2) It is strongly recommended that employees do not post any personal information online such as address, date of birth or financial details, in order to protect their identity.

3) Messages should not be regarded as private if security settings are not set correctly. If messages are to be posted which are not intended for public viewing, the settings should be adjusted so all content is private to the selected group of people. For example on Facebook, the "friends only" setting ensures the audience is limited and access to the personal profile is controlled.

4) Employees should be aware of the nature of the photographs they upload onto social networking sites and consider whether they are appropriate in relation to their professional role. This includes other users posting a photo of the employee which may lead to comments being posted in a wider arena. Employees should be aware that they can be 'tagged' in a photo, and the photo can then be uploaded onto the site without the individual's permission. If this occurs and the photo and / or subsequent comments are inappropriate, the employee should request that the material is removed by the user who posted the initial image.

5) If employees do not wish work colleagues to see their posts, they should not be added as friends.

6) Employees should not give people who are not known to them access to their information. The employee may without realising, be giving access to their personal profile and web pages to people who may know the employee or who are looking for information connected with the employee or the Trust / Academy.

7) Even though employees may not directly identify names of colleagues or the Trust as the employer, people accessing sites may be aware of where employees work and will therefore link any comments and views, expressed about work or otherwise, with the Trust and its employees.

8) The internet is a widely used public forum, and when statements or posts are made on websites they can be irreversible.

9) Even restricted settings do not guarantee a post or comment will not be circulated to, or read by someone who was not intended to see it; and who may take offence at the contents despite not having direct access to the information.

10) The usual signs that help employees avoid offence such as body language are not available online, and it is easy to make 'throwaway' comments in jest which may be misinterpreted, taken seriously and considered offensive.

11) Copyright laws still apply online. Do not use images to which you do not hold the copyright. Information shared should be attributed to the source.

Appendix F

Responsibilities as an employee of the Trust / Academy

Posting information into a public area has the potential of directly/indirectly impacting on the workplace. Employees publishing comments on any site or in any forum to which members of the public may have access should be careful to abide by the following rules:

1) Employees should ensure that online activities do not bring the Trust / Academy into disrepute or adversely affect the employee's position within the Trust / Academy.

2) Employees must not make derogatory comments about the Trust / Academy, or past and present colleagues which may damage the Trust's / Academy's reputation and / or the individual's.

3) Whilst people may seek to use these sites to 'let off steam' employees must avoid saying anything in the heat of the moment or make complaints, which may undermine the Trust's / Academy's decisions and create a poor impression of the Trust's / Academy's principles, standards and work undertaken by the Trust / Academy.

4) Employees must not make statements which may have a negative or damaging effect on working relationships.

5) Employees should not engage in any online communication with colleagues, pupils, their families or other relevant person, which may amount to bullying and harassment; nor should employees make unwanted or unwelcome online communications to those who do not wish to receive them. This includes posting comments about colleagues, pupils or their families in public forums to which they, their friends, family, neighbours or colleagues might have access.

6) Employees should not post gossip or circulate rumours about the Trust / Academy or past or present colleagues, as this will almost always adversely affect the impression of the Trust / Academy, as well as damaging the reputation of individuals and the Trust / Academy.

7) Any information which is posted online should not contradict information provided formally by the Trust / Academy or contradict the effect of a Trust / Academy policy in force.

8) Employees should make it clear that any views expressed are their own and do not reflect the views of the Trust / Academy, the post should not identify the employee as a representative of the Trust / Academy expressing views which are related to work.

9) The Trust values diversity and has pupils and staff from a wide range of backgrounds. Employees should not post offensive or discriminatory remarks

which may lead to concern with regard to the suitability of the post-holder, as they are required to behave in a manner compatible with the Trust's equal opportunities policies. Employees should also not post material that may lead to concern regarding the ability of the employee to commit to the Trust's expectations, standards and policies.

10) Employees should be careful not to join or be associated with online groups which, due to their content or objectives, are incompatible with the policies and objectives of the Trust / Academy.

11) Confidential information about the Trust / Academy should not be posted. This may include aspects of Trust / Academy policy or details of internal discussions about work or colleagues.

12) Employee's email address or work numbers should not be included on personal online profiles or otherwise posted online.

13) Privacy of colleagues and pupils should be maintained at all times.