14.5

Social Media Policy

Statement of intent

St Chads Community Project understands that social media is a growing part of life outside of the organisation. We have a responsibility to safeguard our children and young people against potential dangers when accessing the internet at the Project, and to educate our children and young people about how to protect themselves online when outside of the Project.

We are committed to:

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

Legal framework

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

- DfE (2018) 'Data protection: a toolkit for schools'
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- The Freedom of Information Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

This policy operates in conjunction with the following organisation policies:

- Online Safety Policy
- Data Protection Policy
- Complaints Procedures Policy
- Anti-bullying Policy
- Allegations of Abuse Against Staff Policy
- Photography Policy
- Acceptable Use Agreement
- Confidentiality Policy
- Child Protection and Safeguarding Policy
- Disciplinary Policy and Procedures
- Behavioural Policy

Roles and responsibilities

The Chief Executive Officer is responsible for:

- The overall implementation of this policy and ensuring that all staff, volunteers, parents, clients, children and young people 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.
- 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.
- In conjunction with the Trustees, handling complaints regarding this policy and its provisions in line with the organisation'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.
- Ensure appropriate security measures are implemented and compliance with UK GDPR.

The Trustees are responsible for:

- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.

Staff members and volunteers are responsible for:

- Adhering to the principles outlined in this policy and the Technology Acceptable Use Agreement – Staff and Volunteers.
- Ensuring children and young people adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the setting.
- Reporting any social media misuse by staff, volunteers, client's, children, young people or parents to the Chief Executive Officer immediately.
- Attending any training on social media use offered by the organisation.

Parents are 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 online safety meetings held by the charity wherever possible.
- Not engaging in activities involving social media which might bring the charity into disrepute.
- Not representing their personal views as those of the charity on any social medium.
- Acting in the best interests of pupils when creating, participating in or contributing to social media sites.

Children and young people are responsible for:

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

The communications staff members are responsible for:

- Monitoring and reviewing all organisation-run social media accounts.
- Vetting and approving individuals who wish to be 'friends' or 'followers' on the organisation'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 organisation.
- Handling inappropriate comments or abuse posted on the organisation's social media accounts, or regarding the organisation.
- 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.

ICT technician contractors are responsible for:

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

Definitions

For the purpose of this policy, the organisation defines **"social media"** as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs
- Online discussion forums, such as NetMums
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as Twitter

For the purpose of this policy, **"cyberbullying"** is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.

For the purpose of this policy, **"members of the organisation community"** are defined as any Trustee, member of staff, support staff, Trainee, Apprentice, volunteer, client, child, young person, parent of a child or young person, who have been involved with the organisation past or present.

Data protection principles

The organisation will obtain consent from children, young people and 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 St Chads Community Project accounts – staff, Volunteers, clients, children, young people and parents are not permitted to post any imagery or videos on personal accounts.

Where a child or young person is assessed by the organisation to have the competence to understand what they are consenting to, the organisation will obtain consent directly from that child or young person; otherwise, consent is obtained from whoever holds parental responsibility for the child or young person.

A record of consent is maintained throughout the academic year, which details the children and young people for whom consent has been provided. The Line manager is responsible for ensuring this consent record remains up-to-date.

Parents, children and young people are able to withdraw or amend their consent at any time. To do so, parents, children and young people must inform the organisation in writing. Where parents, children or young people 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' childs' or young persons' requirements following this. Wherever it is reasonably practicable to do so, the organisation 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 child or young person are permitted to be posted, and not videos. This will be made explicitly clear on the consent from provided. The organisation will only post images and videos of children and young people for whom consent has been received.

Only organisation-owned devices will be used to take images and videos of the organisation community, which have been pre-approved by the online safety officer for use. Only appropriate images and videos of children and young people will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.

When posting on social media, the organisation will use group images or videos with general labels, e.g. 'sports day'.

When posting images and videos of children and young people, the organisation will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a child or young person being identified. The organisation will not post children or young peoples' personal details on social media platforms and children and young peoples' 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 child or young person and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a child or young person.

Any breaches of the data protection principles will be handled in accordance with the organisations's Data and Cyber-security Breach Prevention and Management Plan.

Staff social media use

Organisation accounts

The organisation's social media sites will only be created and monitored by the communications officer and other designated staff members. There will be a strong pedagogical or business reason for the creation of social media accounts on behalf of the organisation; official organisation profiles and accounts will not be created for trivial reasons.

If members of staff wish to create a new social media account, they will complete the Social media site creation approval form and return it to the communications officer, who will approve it with the Chief Executive Officer and then create the account on the behalf of the

requesting individuals. The communications officer will be consulted about the purpose of the proposed site and its content.

An organisation social media account will be entirely separate from any personal social media accounts held by staff members and will be linked to an official organisation email account.

Consideration will be given to the following aspects:

- The purpose for using social media
- Whether the overall investment will achieve the pedagogical aim
- The level of interactive engagement with the site
- Whether children, young people, staff, volunteers, parents, clients 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 proposed site
- A clear plan which outlines aspects such as how long the site will last
- How the success of the site will be evaluated.

Organisation social media passwords are kept in the Chief Executive Officer's office - these are not shared with any unauthorised persons, including children and young people, unless otherwise permitted by the Chief Executive Officer. Staff will adhere to the data protection principles outlined in section – Data Protection Principles of this policy at all times.

Staff will ensure any posts are positive in nature and relevant to children and young people, the work of staff and volunteers, groups, activities, events, the organisation or any achievements. Staff will not post any content online which is damaging to the organisation or any of its staff, volunteers, clients, children or young people.

All content expressed on organisation's social media accounts will not breach copyright, data protection or freedom of information legislation.

Staff will ensure the Chief Executive Officer has checked the content before anything is posted on social media. If staff wish for reminders to be posted for parents, e.g. returning slips for a charity trip, staff will seek permission from the Chief Executive Officer before anything is posted.

If inappropriate content is accessed online, a report form will be completed and passed on to the Chief Executive Officer. The Chief Executive Officer retains the right to monitor staff members' internet usage in line with the Data and Cyber-security Breach Prevention and Management Plan.

The organisation's social media accounts will comply with site rules at all times, particularly with regards to the minimum age limit for use of the site. It will be noted that each networking site has their own rules which must be followed – the line manager will induct staff to each new social media platform, providing them with the relevant training and information.

Personal accounts

Staff members and volunteers will not access personal social media platforms during working hours, but they are permitted to use social media during break times. Staff and volunteers will avoid using social media in front of children young people and clients.

Staff members and volunteers will not use any organisation-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the Chief Executive Officer. Staff and volunteers are not permitted to use the organisation's WiFi network to access personal accounts, unless otherwise permitted by the Chief Executive Officer, and once the Chief Executive Officer has ensured the necessary network security controls are applied.

Staff and volunteers will not 'friend', 'follow' or otherwise contact children, young people, parents or clients through their personal social media accounts. If children, young people, parents or clients attempt to 'friend' or 'follow' a staff member or volunteer, they will report this to the Chief Executive Officer.

Staff members and volunteers will not provide their home address, phone number, mobile number, social networking details or email addresses to children, young people, parents or clients – any contact will be done through authorised organisation contact channels. Staff members and volunteers will use their organisation email address for St Chads Community Project business and personal email address for their private correspondence; the two should not be mixed.

Staff members will ensure the necessary privacy controls are applied to personal accounts and will avoid identifying themselves as an employee or volunteer of the organisation on their personal social media accounts. Where staff members and volunteers use social media in a personal capacity, they will ensure it is clear that views are personal and are not those of the organisation.

No staff member or volunteer will post any content online that is damaging to the organisation or any of its staff, volunteers, children, young people or clients. Staff members and volunteers will not post any information which could identify a child, young person, client, group or the organisation – this includes any images, videos and personal information. Staff and volunteers will not take any posts, images or videos from social media that belong to the organisation for their own personal use. Staff members and volunteers will not post anonymously or under an alias to evade the guidance given in this policy.

Breaches of this policy by members of staff or volunteers 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 and volunteers will be aware that if their out-of-work activity brings the organisation into disrepute, disciplinary action will be taken.

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

Social media will not be used as a platform to attack, insult, abuse or defame children, young people, clients, their family members, colleagues or other professionals.

Staff members and volunteers' personal information will not be discussed on social media.

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 organisation.

Parents will be asked not to share any photos or personal details of children or young people when commenting on the organisation social media sites, nor post comments concerning other children, young people, staff members, volunteers or clients 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 Chief Executive Officer, 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.

Children and young people social media use

Children and young people will not access social media during sessions and activities in the Project, unless it is part of a structured activity. Children and young people are not permitted to use the organisation's WiFi network to access any social media platforms unless prior permission has been sought from the Chief Executive Officer, and they have ensured appropriate network security measures are applied.

Children and young people will not attempt to 'friend', 'follow' or otherwise contact members of staff or volunteers through their personal social media accounts. Children and young people are only permitted to be affiliates of the organisation social media accounts. Where a child, young person or parent attempts to "friend" or 'follow' a staff member or volunteer on their personal account, it will be reported to the Chief Executive Officer.

Children and young people will not post any content online which is damaging to the organisation or any of its staff, volunteers or peers. Children and young people will not post anonymously or under an alias to evade the guidance given in this policy.

Children and young people are instructed not to sign up to any social media sites that have an age restriction above their age.

If inappropriate content is accessed online on the organisation's premises, it will be reported to a member of staff.

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

Online safety

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

Concerns regarding a staff member's online behaviour will be reported to the Chief Executive Officer, who will decide on the best course of action in line with the relevant policies, e.g. the Staff Handbook, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the Chief Executive Officer, it will be reported to the chair of Trustees.

Concerns regarding a Child or young person's online behaviour will be reported to the DSL, who will investigate any concerns with relevant staff members, e.g. the CEO and ICT technicians, and manage concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Chief Executive Officer will contact the police. The organisation will avoid unnecessarily criminalising children and young people, 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 child 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 Child Protection and Safeguarding Policy.

Blocked content

In accordance with the organisation's Data and Cyber-security Breach Prevention and Management Plan, the ICT Technician will install firewalls on the organisation's network to prevent access to certain websites in the childcare setting. The following social media websites are not accessible on the childcare setting's network:

- Twitter
- Facebook

- Instagram

The Chief Executive Officer and ICT Technician retains the right to monitor staff, volunteer. Children and young people's access to websites when using the organisation's network and on St Chads Community Project-owned devices.

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

Inappropriate content accessed on the organisation's computers will be reported to the Chief Executive Officer and ICT 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 the Line manager which will be approved by the Chief Executive Officer.

Cyberbullying

Cyberbullying incidents are taken seriously at St Chads Community Project. Any reports of cyberbullying on social media platforms by Children or young people will be handled in accordance with the Anti-bullying Policy.

Cyberbullying against children, young people, staff, volunteers or clients 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 or volunteers will be handled in accordance with the Allegations of Abuse Against Staff Policy.

Training

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

Children and young people in our setting will be educated about online safety and appropriate social media use on a regular basis through a variety of mediums, including group discussions, activities. Children and young people 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 children, young people, staff, volunteers, clients and parents will be refreshed in light of any significant incidents or changes.

Monitoring and review

This policy will be adopted on 1st June 2022 by the Chief Executive Officer and Board of Trustees.

The next scheduled review date for this policy is June 2025.

Any changes made to this policy will be communicated to all staff, volunteers, children, young people, parents and clients.

Blocked content access request form

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

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 Line Manager	
Action taken:	
Staff name:	
Date:	
Signature:	

Social media site creation approval form

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

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		
☐ Children of the organisation Ages:	☐ Organisation staff	☐ Children's family members
☐ External organisations	☐Groups or clubs	☐ Members of the public
☐ Other (please give details)		
Proposed contributors to the site		
☐ children of the organisation Ages:	☐ Organisation staff	☐ Children's family members
☐ External organisations	☐ Groups or Clubs	☐ 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 children & young people, 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 Chief Executive Officer.		
Line manager I approve the aims and content of the proposed site and the use of the charity brand and logo.	Name:	
	Signature:	
	Date:	
Chief Executive Officer I approve the aims and content of the proposed site and the use of the school brand and logo.	Name:	
	Signature:	
	Date:	

Photography, Video and Social Media Parental Consent Form

This consent form explains the reasons why and how St Chads Community Project may use images and videos of your child. It also provides information pertaining to how St Chads Community Project wishes to use personal data on social media, details the terms under which the organisation will use this data and requests consent for the organisation to use your personal data on social media.
Please read the form thoroughly and outline your agreement as appropriate.

Childs Full Name:

Why Do We Need Your Consent?

We request 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, St Chads Community Project 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, we will abide by the conditions you outline in this form.

Why Do We Use Images and Videos of Your Child and Why Will We Be Using Personal Data on Social Media?

We use images and videos of children as part of displays to promote the positive and inclusive ethos of the charity; to celebrate the achievements of children; to promote the charity on social media and on the charities website; and for other publicity purposes in printed publications, such as newspapers.

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

If, for example, a child 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 we may use personal data, take images or videos of individual children or groups of children to use on social media, the charities website, in the charities prospectus and other printed publications, such as a newsletter.

Who Will Be Able to See The Data Once It Is On Social Media?

The charities social media platforms are in the public domain. Please note, once stories, data, images or videos have been posted onto social media platforms, the content which has been posted can be shared, this means 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/ carers to inform the charity, in writing, if consent needs to be withdrawn or amended.

- The charity will not use personal details or full names of any child in an image or video on our website, social media, in our charity prospectus or any other printed publications.
- The charity will not include personal emails, postal addresses, or telephone numbers on images or videos on our website, social media, in our charity prospectuses or any other printed publications.
- The charity may use pictures of children or staff that have been drawn by children.
- The charity may use or post pictures of work created by children on social media.
- The charity may use group images or videos of children with general labels, e.g. 'sports day'.
- The charity will only use images and videos of children who are suitably dressed, i.e. it would not be suitable to display an image of a child in swim wear.
- The charity 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 section.

The charity will only publish and post personal data, images and videos of your child for the conditions that you provide consent for.

I Provide Consent To:		
	Yes	No
The charity photographing my child.		
The charity videoing my child.		
The charity using images of my child on the charity website.		
The charity using videos of my child on the charity website.		
The charity using images of my child on social media, including but not limited to: Twitter, Facebook, Instagram.		
The charity using videos of my child on social media, including but not limited to: Twitter, Facebook, Instagram.		
The charity using my child's first name on social media.		
The charity using my child's age on social media.		
The charity using images of my child in marketing material, e.g. in the newsletter or prospectus.		

Refreshing Your Consent

This form is valid for the entire academic year. Parents are required to fill in a new form for their child every September.

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 children's images and videos.
- Changes to a child's circumstances – e.g. safeguarding requirements mean a child'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 Head of children Services. 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, images or videos that was shared prior to withdrawal; however, the charity will make every effort to remove posts about your child where possible e.g. images of the child on social media will be removed. If you would like to withdraw your consent, you must submit your request in writing to the Head of Children Services.

Declaration	
I understand: • Why my consent is required. • The reasons why St Chads Community Project uses images and videos of my child. • The reasons why St Chads Community Project uses my child's personal data on social media. • Who will be able to view my child's personal data once posted on social media. • The conditions under which the charity uses images and videos of my child. • The conditions under which the charity uses personal data of my child on social media. • I have provided my consent above as appropriate, and the charity will use images and videos of my child in line with my requirements. • Consent is refreshed on an annual basis every September and I must re-provide consent in subsequent years. • I will be required to re-provide consent where any circumstances change. • I can amend or withdraw consent at any time and must do so in writing to the Head of Children Services.	
Full name of Parent/ Carer:	
Signature:	Date:

Version 1
Adopted June 2022