

St Charles' Catholic Voluntary Academy

Acceptable Use of the Internet and Social Media



Definitions

- Must - An absolute requirement
- Must Not - An absolute prohibition.
- Should - There may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- Should Not - There may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing.

May –Optional

Our Vision

The St Charles' way is for every child to: 'Belong, Believe and Blossom'

Rationale

Social media use is increasing worldwide, particularly in the younger generations. We believe it is our duty as a school to harness the opportunity we have to lead from the front and educate our children on best practice and how to stay safe online.

We foster the mentality that everything should be open, transparent and public. Despite many social networks having the option to become private channels, we're fully aware that nothing online is truly private and we strive to educate our children on this viewpoint.

Our school channels are all public channels. We don't believe in closed or private groups, as this fosters the mentality of it being okay to have private conversations online, which goes against what we teach our children with regard to online safety and talking to strangers.

Our Aims

We have three core aims for using social media within school and every action we take should be to support one or more of these aims. They are:

- To increase engagement between the school and parents/carers.
- To lead from the front and educate our children on best practice when using social media.
- To share and promote our school in a positive light to prospective parents and the wider community.
 - To ensure all pupils Belong, Believe and Blossom and use social media in an appropriate and safe manner.

Social Networks We Use In School

There are many different social networks, each with a different mission, potential audience and uses. It is unrealistic to assume that we should use every single social network as a school – it would be too time consuming and difficult to manage – but we have considered each platform and actively use those that are most suitable for us and our circumstances.

We believe in having a presence on all social networks regardless of whether we actively use them, since this discourages others from creating accounts which mimic or falsely represent our school.

The school will have a presence on the following social network: Twitter. Where possible, the account will be listed as a business or company under the school name, rather than as a personal or individual. It is important for us, as a school, to maintain a presence on these platforms to discourage others from creating a derogatory account in our school name. The school will actively post on the following social network: Twitter.

Usage and Best Practice

To ensure we meet our aims, we have detailed what we consider best practice when using social media within our school. We expect all our employees, pupils and parents to adhere to the statements contained in this policy.

Taking Photographs and Videos

This section applies when capturing any content with a camera or microphone, on any device.

Must (required)

- All children must be made aware a photo/video is being taken prior to doing so. To ensure all children consent to the photo/video being taken and it is public knowledge. This protects the teacher and the children.
- For safety, we have our own 'capture word' which must be said at all times before a photo or video is taken. Our word is '**Smile**'.

This word is iconic to our school and is used to ensure all children know a photo or video is going to be taken.

- There must not be any media taken of a single, identifiable child.

Research suggests that if a child is called by his/her name, then they are more likely to interact with a stranger. To avoid this, we do not identify who the children are in any of our media.

- There must not be any media taken which contains a child with identifiable features, such as name badges, drawers with names etc.

Identifiable features, such as books with stickers on and name badges, contribute to a stranger knowing who a specific child is.

- Audio contained within a video must not contain identifiable children's names.

For the same reasons above, it is important not to provide members of the public with a child's face and their name.

- Employees must not produce media in which children are inappropriately dressed, or contain nudity or profanity.

Besides the obvious, an inappropriate photograph or video could put the child, employee and the school at risk.

Should (recommended)

- When possible, children should be shown the photo or video after it is taken, before it is published online.

Individual children can be identified and so it is always best practice to photograph them in groups.

- Employees should be aware that photos posted online may be resized by the platform they are uploaded to and so should consider what their photo would appear like if it is cropped either at the sides or the bottom.

Many social networks have a default size or ratio in which they upload a photo. For example: Instagram is square.

- Employees should also ensure they consider the backdrop of the photo or video they are taking, ensuring it is tidy, respectable and shows the school in a positive light.

It is not just the foreground of the photo or video which is important, the whole frame may be seen by the public.

- Employees should remain sensitive to any children who appear uncomfortable.
- Children have the right to remain out of any media taken if they feel uncomfortable as there could be a personal issues causing this discomfort.

Posting to Social Media

This section applies when anything is posted to social media from a professional capacity.

Must (required)

- All school related content must be posted to official school accounts only. For reference, a list is contained in this document.

This is to ensure consistency in the content which is published online.

- Employees must not post school related content on any of their personal accounts.

This is to ensure nothing is misconstrued when coming from a member of staff.

- Posts must not contain any identifiable information within the text or media.

For child protection reasons, we don't include anything which may identify a child.

- All posts must be considered public, regardless of where they are posted, and be treated as such.

Regardless of privacy settings, it is always possible for someone to screenshot and share a post or comment.

- Employees must only upload media that they themselves have created and own the IP (intellectual property) to.

To avoid copyright issues, all content must be owned by our school or our employees. If photographs have been taken by an external photographer, the school must obtain the rights to use the photos before they can be published online.

- The school must keep a list of children who do not have parental consent to be online. This must be cross referenced before every post which contains media.

This is to ensure that there are no children posted online who do not have parental consent.

- Employees must not post anything which may bring the school into disrepute or portray the school in a negative light.

All content must be checked to ensure it portrays the school positively.

- Children must not be tagged in photographs.

This is so children cannot be identified.

Should (recommended)

- There should not be any content posted by the school to a private page or closed group.

We do not advocate private conversations or groups online as this goes against what we teach our children in terms of being open and honest, and not to have private conversations with strangers (online or offline).

We do not advocate private conversations or groups online as this goes against what we teach our children in terms of being open and honest, and not to have private conversations with strangers (online or offline).

- Employees should not post about any school related matters on their own personal account. Issues or school matters should be discussed in person, in school, rather than publicly online.
- Employees should ensure that content is checked by another member of the team before posting to ensure the content abides by the rules contained within this policy. Two sets of eyes are far better than one in ensuring content complies with school policy.

May (optional)

- Employees may like, share, favourite, comment (or similar) on school related content that has been published via official school accounts.

This increases engagement with our school accounts and encourages others to interact too.

- Employees may want to consider the time of day they are posting to maximise their audience.

Depending on the audience, people will be active (online) at certain times of the day.

To reach the most people, it is preferable to post at the time when most people are likely to be active.

Engaging with Parents and Pupils

This section applies when the school, or employees, interact with others online via social media.

Must (required)

- Employees must ensure they do not interact or post comments on social networks which may bring themselves or the school into disrepute.
- Employees may not connect with parents/guardians of a pupil currently on roll even if they are known on a personal level.
- All comments must be checked to ensure accuracy and positivity.

Should (recommended)

- Employees should not connect or engage with any pupils on the current school roll via social media.

This is to ensure we keep parents and children safe. Unfortunately, engaging with pupils online can often be misconstrued.

- Employees should only engage with parents, pupils (where applicable) and the public with regard to school matters via official school accounts. This is to ensure consistency with messages and responses from the school.

May (optional)

- Employees may engage and reply where possible via the official school accounts to increase engagement with others.

This encourages others to interact and ultimately increases the reach (amount of people who see the post, profile or page).

- Employees may share the content posted to official school accounts on their own accounts if they wish to.

As the content is already in the online domain, there is no reason why an employee cannot then share the original post.

Passwords and Security

This section applies to the security of school accounts and personal accounts.

Must (required)

- Passwords to school social media accounts must remain safe and secure at all times. The Head and the Deputy Head are the only people with these passwords.

To avoid potential misuse or intrusion from unauthorised people.

- Passwords must not be shared between employees. Sharing passwords means actions are not then fully accountable to one person. A password per person is advised for this reason.

May (optional)

- Employees may want to set up two factor authentication on their social media accounts for added security.

Two factor authentication ensures that when an account is accessed from a new device or browser, the user must enter a code which is sent to their personal mobile phone first. This stops unauthorised access.

Intellectual Property (IP)

This section applies to all media created by employees at the school.

Must (required)

- All media posted must be owned by the person uploading, or the organisation they work for, before it is uploaded.

To avoid copyright issues, we must own the content ourselves.

- Unless stated otherwise in an employment contract, all media and IP (intellectual property) remains the property of the person who created it. By posting it to a school account, employees give the school permission to share (copy and redistribute the material in any medium or format) and adapt (remix, transform, and build upon the material) the media.

This is to ensure we are allowed to share or adapt any content created by our employees.

Personal Accounts on Social Networks

This section applies to employees who use social media in a personal capacity.

Must (required)

- Employees must not attempt to impersonate the school through an unofficial or spoof account. Spoof accounts are not a realistic or accurate representation of the school.

Should (recommended)

- Employees should always treat their personal account posts as public, even if an account has privacy settings enabled which state otherwise.

Posts can always be screenshotted and shared, which means nothing is ever really private.

May (optional)

- Employees may have personal accounts on any social networks they choose. Social networks were initially created for personal use, so it would be unreasonable of us to enforce a 'do not use' policy for our employees.

Using Personal Devices in School

This section applies to employees who bring, carry, store or use a personal electronic device in school.

Must (required)

- Only the Head, Deputy and RE Subject Leads are authorised to use personal devices to capture content for school use. This content must be immediately removed from personal devices once uploaded.

This is to ensure that any content cannot be copied or removed from the device easily by another person.

- Any school content kept on a personal device must only be kept for the minimum amount of time feasible, up to a maximum of 24 hours.

This is to minimise the risk of someone with malicious intent getting hold of school content.

Should (recommended)

- If personal devices are used, the pin or password should be changed at least every 90 days.

This is standard for anyone with passwords or pins on devices to maximise security.

Parental Responsibilities

This section applies to parents who access official school channels on social media.

Must (required)

- Parents must treat all interactions with an official school account as public.

Depending on how the social network is managed, it is possible that multiple employees may have access to the account. For sensitive subjects, it is recommended that parents seek answers via a different means and speak to the school directly.

- In line with our zero tag approach, parents must not tag children or other parents in photographs, or knowingly publicly identify a child.

Identified children are at risk from child predators on the streets if they know their names.

Should (recommended)

- Parents should always keep in mind that their posts and interactions are public.

As everything can be screenshotted or shared, there is no such thing as a private post.

- Parents should choose the most appropriate method of communication with the school depending on the matter in which they wish to discuss.

There are many communication methods open for parents to use which may be more suitable than online, including; visiting school, phone and email.

- Parents should not expect a response from questions or comments posted on social media accounts.

Due to the nature of social media, messages and comments can sometimes be missed.

May (optional)

- Parents may interact, comment and share content posted on school official accounts as often as they wish.

Interacting with posts increases engagement and ultimately means our posts are seen by more people.

- Parents may invite others to like, follow, or equivalent, any of the school official accounts.

The more people who follow or like our school accounts, the more people see our posts.

Pupil Responsibilities

This section applies to pupils who have their own accounts on social networks.

Must (required)

- Pupils must not tag themselves or others in school photos. Identifying people who may not wish to be identified online can be a security risk.
- Pupils should only have accounts on social networks if they comply with the sites age restriction.

All social networking sites have a lower age limit due to the nature of the site and type of content likely to be seen.

- Pupils should not post anything on an official school account which may portray the school in a negative light.

Derogatory comments are offensive and may cause the school, staff or other pupils harm.

Non-Compliance

- Any breach of this policy, particular attention is drawn to those statements which are outlined as being 'required/must', may lead to disciplinary/legal action being taken against those involved, in line with the school's disciplinary procedures.
- The school will act as immediately as possible on any incidents where the safety of children, employees or parents is at risk.
- The school reserves the right to remove, ban and block any user, comment or photo shared by another person to our official school accounts if it is offensive or inappropriate.

Curriculum Delivery

Teaching pupils about E-Safety and online safety is integral part of our curriculum and the school launched 'Charlie's Cyber Club' supported by National Lottery money in March 2020.

Further Information

This policy is to be read in conjunction with:

E-Safety Policy

Staff Code of Conduct

Behaviour Policy/Anti-Bullying/Cyber Bullying

Safeguarding and Child Protection Policy

PSHE Policy

Useful Websites

Think You Know

NSPCC

CEOP

UK Safer Internet

Action for Children

Bitesize

www.childnet.com

Child line online

Nationalonlinesafety.com

Misuse and Complaints

If you feel that this policy is not being followed in some way, please let us know by contacting the school at info@st-charles.derbyshire.sch.uk.

Date: 17th June 2020

Policy Review Date: June 2021

Signed:

Signed: