St Bede's Catholic School & Byron Sixth Form College

Online Safety Policy

Approved by:	Local Governing Body	**Date:**	
Last reviewed on:			
Next review due by:			

The purpose of this policy

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in the activities of St Bede's Catholic School & Byron Sixth Form College.

We believe that our students:

- should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.
- should never experience abuse of any kind.

We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that the young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep students safe online, whether or not they are using our network and devices
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

How we work together to keep everyone safe:

The Online Safety Coordinator will:

- provide clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- provide support, information and encouragement for parents and carers to do what they can to keep their children safe online
- develop an online safety agreement for use with young people and their parents/carers
- provide annual assemblies for each year group to maintain the high profile of positive approaches to online safety and update awareness of issues that can arise when living and learning online
- provide supervision, support and training for staff and volunteers about online safety
- develop clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person.

ICT Support Staff will:

- review and update the security of our information systems regularly
- perform weekly checks of the active monitoring system logs and record any concerns
- identify when major issues are developing and report them to the head of safeguarding
- ensure devices connected to the school network utilise a filtered connection (Smoothwall) that blocks access to inappropriate content and logs attempts to access it
- ensure personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate

Teaching Staff will:

- ensure that usernames, logins, email accounts and passwords are used effectively

- ensure that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given

- examining and risk assessing any social media platforms and new technologies before they are used within the organisation

- support and encourage young people to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others.

If online abuse occurs, we will respond to it by:

- Invoking our safeguarding procedures to provide an immediate response to abuse (including online abuse)

- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation

- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account

- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Related policies and procedures:

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding & Child protection.

- Dealing with allegations of abuse made against a child or young person.

- Managing allegations against staff and volunteers.

- Code of conduct for staff and volunteers.

- Anti-bullying policy and procedures.

- Photography and image sharing guidance.

Contact details

Online safety co-ordinator

Name: Mrs J Jenkin

Phone/email: 0191 5876220 / j.jenkin@st-bedes.durham.sch.uk

Senior lead for safeguarding and child protection

Name: Mrs J Jenkin

Phone/email: 0191 5876220 / j.jenkin@st-bedes.durham.sch.uk

ICT support staff with responsibility for online safety

Name: Mr D Oxley

Phone/email: 0191 5876220 / enquiries@st-bedes.durham.sch.uk

Student Acceptable Use Agreement

I will maintain my privacy by:

1. Keeping my passwords private

2. Check my privacy settings are set appropriately

3. Not sharing personal information

4. Keeping my passwords safe and private to protect my privacy, schoolwork and safety

I will keep myself safe by:

1. Making sure that my internet use is safe and legal, and I am aware that online actions have offline consequences

2. Complying with the school's acceptable use policy as I know that my use of computers, devices and internet access will be monitored to check that I do

I will demonstrate I am responsible by:

1. Not accessing or changing other people files, accounts or information

2. Only uploading appropriate pictures or videos of others online when I have permission

3. Keeping personal devices turned off and out of sight during lessons

4. Treating the academy's systems and equipment with respect

5. Only using school devices and internet access to help me with my learning. If I'm not sure if something is allowed, I will ask a member of staff

6. Writing emails and online messages carefully and politely

7. Only changing the settings on devices provided by the school if a teacher/technician has said I can

8. Making no attempt to bypass internet filters. They are there to protect me.

9. Never using the school's systems for personal financial gain, gambling, political purposes or advertising

I will demonstrate I am kind by:

1. Never engaging in bullying behaviour in any form (on and offline)

2. Not sharing any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school's community.

I will demonstrate I am reliable by

1. Always checking that any information I find online is reliable and accurate.

2. Reporting anyone trying to misuse technology to a member of staff.

3. Speaking to an adult I trust if something happens to either myself or another student which makes me feel worried, scared or uncomfortable.

4. Keeping up to date with issues I may face online I will visit the following to find out more about keeping safe online;

www.thinkuknow.co.uk,

www.childnet.com

www.childline.org.uk

Agreement

1. I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages.
2. I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources.
3. I understand that it may be a criminal offence or breach of the academy's policy to download or share inappropriate pictures, videos or other material online.
4. I know that If the teachers or ICT support staff suspect that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones and other devices.
5. I know that if I do not follow this agreement then I will be subject to sanctions.
6. I have read and talked about these rules with my parents/carers.

I have read, understood and agreed to comply with St Bede's Catholic School & Byron Sixth Form College Student Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of student: ……………………………………………………………………………

Signed: ……………………………………………………………………………………………………

Date (DDMMYY): ……………………………………………………………………………………..

Adults in School Acceptable Use Agreement

Policy Scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within St Bede's Catholic School & Byron Sixth Form College both professionally and personally. This may include use of devices and email as well as IT networks, data and data storage and online and offline communication technologies.

2. I understand that this Acceptable Use of Technology Policy (AUP) should be read and followed in line with the staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the academy ethos, staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Academy Devices and Systems

4. I will only use the equipment and internet services provided to me by the school for example laptops, tablets, mobile phones and internet access, when working with students.

5. I understand that any equipment and internet services provided by the academy are intended for educational use and should only be accessed by members of staff.

Reasonable personal use of setting IT systems and/or devices by staff is/is not allowed.

Data and System Security

6. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

- I will use a 'strong' password to access the school systems.

- I will protect the devices in my care from unapproved access or theft.

7. I will respect school’s system security and will not disclose my password or security information to others.

8. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

9. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

10. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies.

- All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely

- Any data being removed from the academy site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the ICT support team

11. I will not keep documents which contain academy related sensitive or personal information, including images, files, videos and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school remote platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

12. I will not store any personal information on the academy IT system, including school laptops or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

13. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material;

to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

14. I will not attempt to bypass any filtering and/or security systems put in place by the school's.

15. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider/Team/lead (named contact) as soon as possible.

16. If I have lost any school related documents or files, I will report this to the ICT Support Provider/Team/lead (named contact) and academy Data Protection Officer (name) as soon as possible.

17. Any images or videos of students will only be used as stated in the school camera and image use policy. I understand images of students must always be appropriate and should only be taken with school provided equipment and taken/published where students and their parent/carer have given explicit consent.

Classroom Practice

18. I am aware of safe technology use in the classroom and other working spaces, including appropriate supervision of students, as outlined in the school online safety policy.

19. I have read and understood the school online safety policy which covers expectations for students regarding mobile technology and social media.

20. I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used on site.

- creating a safe environment where students feel comfortable to say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.

- involving the Designated Safeguarding Lead or a Deputy Designated Safeguarding Lead as part of planning online safety lessons or activities to ensure support is in place for any students who may be impacted by the content.

- make informed decisions to ensure any online safety resources used with students is appropriate.

21. I will report any filtering breaches (such as access to illegal, inappropriate or harmful material) to the DSL in line with the academy online safety/child protection policy.

22. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text or music are protected, I will not copy, share or distribute or use them.

Use of Social Media and Mobile Technology

23. I have read and understood the academy's online safety policy which covers expectations regarding staff use of mobile technology and social media.

24. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role and in line with the staff behaviour policy/code of conduct, when using school and personal systems. This includes my use of email, text, social media and any other personal devices or mobile technology.

- I will take appropriate steps to protect myself online when using social media as outlined in the online safety/social media policy

- I am aware of the academy's expectations with regards to use of personal devices and mobile technology, including mobile phones as outlined in the online safety policy.

 I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media.

 I will ensure that my use of technology and the internet does not undermine my professional role or interfere with my work duties and is in accordance with the academy behaviour policy/code of conduct and the law.

25. My electronic communications with current and past students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

 I will ensure that all electronic communications take place in a professional manner via academy approved and/or provided communication channels, such as a school email address or telephone number.

 I will not share any personal contact information or details with students, such as my personal email address or phone number.

 I will not add or accept friend requests or communications on personal social media with current or past students and/or parents/carers.

 If I am approached online by a student or parents/carer, I will not respond and will report the communication to my line manager and the Designated Safeguarding Lead (DSL).

 Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or Headteacher/line manager.

26. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the DSL and/or the Headteacher/line manager.

27. I will not upload, download or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience or needless anxiety to any other person.

29. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the academy into disrepute.

Policy Compliance

30. I understand that the academy may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

Policy Breaches or Concerns

31. I will report and record concerns about the welfare, safety or behaviour of students or parents/carers to the DSL in line with the academy online safety/child protection policy.

32. I will report concerns about the welfare, safety or behaviour of staff to the Headteacher/line manager, in line with the allegations against staff policy.

33. I understand that if the school believes that unauthorised and/or inappropriate use of their systems or devices is taking place that disciplinary procedures will be invoked as outlined in the staff behaviour policy/code of conduct.

34. I understand that if the school believes that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with St Bede's Catholic School & Byron Sixth Form College Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

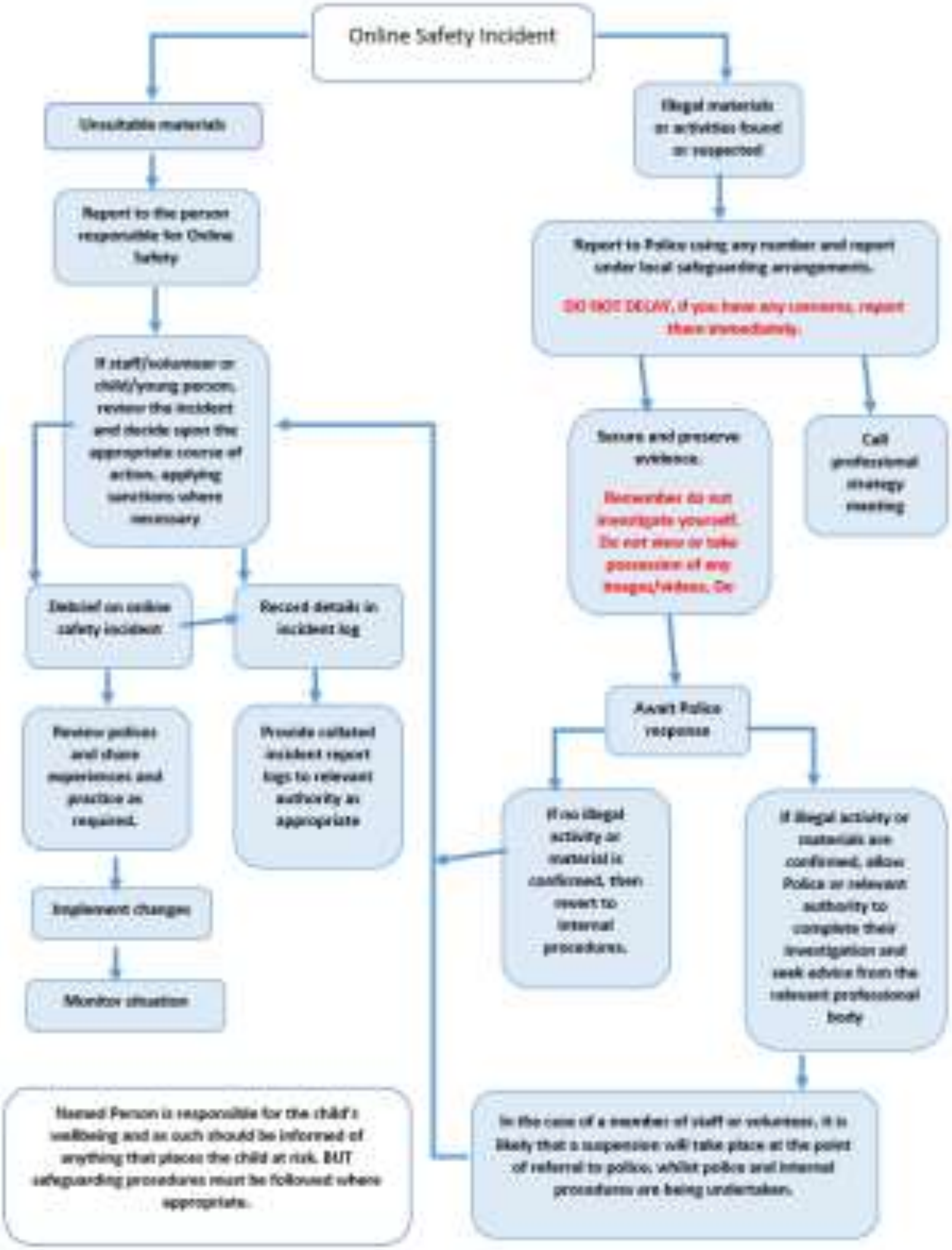
Name of staff member: ………………………………………………………………………

Signed: ……………………………………………………………………………………………………..

Date (DDMMYY): ……………………………………………………………………………………..

Incident Response Procedure

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review policies and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

Scope

This policy is subject to the school's codes of conduct and acceptable use agreements. This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school

The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

Digital communications with students are also considered. Staff may use social media to communicate with students via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Roles & Responsibilities

SLT will:

- Facilitate training and guidance on Social Media use
- Develop and implement the Social Media policy
- Taking a lead role in investigating any reported incidents
- Make an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
- Approve account creation

Administrators/Moderators of SM accounts will:

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Teaching Staff will:

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training

- Regularly monitoring, updating and managing content he/she has posted via schools accounts

- Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

St Bede’s have whole-school and departmental social media accounts. No other accounts should be created. If a member of staff feels that additional accounts are necessary, they should present a business case to the Leadership Team which covers the following points:

- The aim of the account

- The intended audience

- How the account will be promoted

- Who will run the account (at least two staff members should be named)

- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on an school social media account.

Behaviour

 The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

 Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

 Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

 If a journalist makes contact about posts made using social media staff must refer this straight to SLT.

 Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

 The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

 The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and

other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

 Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.

 Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

Tone

- The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:
- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

The school recognises that sharing of images can have a positive impact on raising its profile online and celebrating its successes with parents and the wider community. The use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be

appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

By Staff

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- The school permits reasonable and appropriate access to private social media sites.

By Students

- Staff are not permitted to follow or engage with current or prior students of the academy on any personal social media network account

- The school's education programme seeks to enable the students to be safe and responsible users of social media

- Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the /school's behaviour policy.

By Parents/Carers

 If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.

 The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website / social media and regular sessions to update parents on how best to support their children.

 Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school. The school should effectively respond to social media comments and reviews made by others according to a defined policy or process.

 Managing your personal use of Social Media and keep yourself safe by: Adopting the adage that "Nothing" on social media is ever truly private

 Not using the academy logo and/or branding on personal accounts

 Not allowing social media to blur the lines between your professional and private life

 Checking your settings regularly and test your privacy

 Keeping an eye on your developing digital footprint

 Keeping your personal information private

 Regularly reviewing your connections – keep them to those you want to be connected to

 Always considering the; Scale, Audience and Permanency of what you post

 Always being polite even if you need to be critical

- Taking control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Knowing how to report a problem

Managing school social media accounts

Anyone given access to manage the school accounts should:

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible
- Consider the appropriateness of content for any audience of school accounts

They shouldn't:

- Make comments, post content or link to materials that will bring the school into disrepute
- Publish confidential or commercially sensitive material
- Breach copyright, data protection or other relevant legislation
- Link to, embed or add potentially inappropriate content
- Post derogatory, defamatory, offensive, harassing or discriminatory content

- Use social media to air internal grievances

This policy document will be reviewed in July 2023