Online Safety Policy

Policy written and reviewed by: Matthew Jones

Named Director with lead responsibility: Richard Dalton

Date written: December 2020

Policy Reviewed: September 2021

Policy Reviewed: September 2022

Policy Reviewed: September 2023

Date of next review: September 2024

This policy will be reviewed <u>at least</u> annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

Grow 19 Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Grow 19, involving staff, learners and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, Teaching Online safety in School 2019, Further Education Operational Guidance 2020 and the Kent and Medway Safeguarding Adults Board procedures.

- The purpose of the Grow 19 online safety policy is to:
    - Safeguard and protect all members of Grow 19 community online.
    - Identify approaches to educate and raise awareness of online safety throughout the community.
    - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
    - Identify clear procedures to use when responding to online safety concerns.

- Grow 19 identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material
    - **Contact:** being subjected to harmful online interaction with other users
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- Grow 19 believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- Grow 19 identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Grow 19 believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
- Anti-bullying policy
- Behaviour policy
- Safeguarding Adults at Risk Policy
- Curriculum Policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. Grow 19 will review this policy at least annually.
    - The policy will also be revised following any national or local policy requirements, any safeguarding concerns or any changes to the technical infrastructure
- Grow 19 will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Principal will be informed of online safety concerns, as appropriate.
- The named DSL will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) has lead responsibility for online safety. The appointed Online Safety Coordinator is Kirstie Hemingway (Principal).
- Grow 19 recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff and learner code of conduct policy and acceptable use policy.
- Ensure that suitable and appropriate filtering systems are in place and work with technical staff to monitor the safety and security of our systems.
- Ensure that online safety is embedded within the curriculum, which enables all learners to develop an appropriate understanding of online safety.
- Support the DSL and Online Safety Coordinator by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside College staff to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.

- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to promote positive online behaviour to learners an the wider community.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate to the Board of Directors.
- Update the Policy annually.
- Meet regularly (termly) with the Director with a lead responsibility for safeguarding and online safety.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by learners.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and Directors, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team *(*including password policies and encryption*)* to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure appropriate access and technical support is given to the DSL to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.5 It is the responsibility of learners (at a level that is appropriate to their ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the learner agreement.
- Respect the feelings and rights of others both on and offline.

- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.

4.6 It is the responsibility of parents and carers to:

- Read the learner agreement and encourage the young person to adhere to it.
- Support our online safety approaches by discussing online safety issues and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that the young person is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if the young person encounters risk or concerns online.
- Contribute to the development of the online safety policies.
- Support the use of our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- Grow 19 will establish and embed online safety in the curriculum to raise awareness and promote safe and responsible internet, social media and phone use amongst learners by:
    - Ensuring education regarding safe and responsible use of technologies is delivered.
    - Including online safety in PSD, Employability and specific tutorials.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
    - Educating learners in the effective use of social media, apps and phones.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5.2 Learners at Risk

- Grow 19 recognises that some learners are more at risk online due to a range of factors. This may include, but is not limited to care leavers, learners with Special Educational Needs and Disabilities (SEND) or mental health needs, learners with English as an additional language (EAL) and learners experiencing trauma or loss.
- Grow 19 will ensure that differentiated and ability appropriate online safety education, access and support is provided to susceptible learners.
- When implementing an appropriate online safety policy and curriculum, Grow 19 will seek input from specialist staff including the Online Safety Coordinator, DSL and other organisations.

5.3 Training and engagement with staff

Grow 19 will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety and safeguarding training for all staff on a regular basis, with at least annual updates. This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

6. Reducing Online Risks

- Grow 19 recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- Grow 19 will:
    - Regularly review the methods used to identify, assess and minimise online risks.
    - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
    - Ensure that appropriate filtering is in place and take all reasonable precautions to ensure that users can only access appropriate material.
    - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community.

7. Safer Use of Technology

7.1 Classroom Use

- Grow 19 uses a wide range of technology. This includes access to:
    - Computers, laptops and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platform/intranet
    - Email
    - Digital cameras, web cams and video cameras
- Learners are encouraged to use their personal mobile phones as a learning, recording and communication tool. Staff are issued with work phones for this purpose and lone working.

- All college owned devices will be used with appropriate safety and security measures in place.
    - Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
    - Grow 19 will ensure that the copying and subsequent use of Internet-derived materials by staff and learners complies with copyright law.
    - Learners will be encouraged to use age-appropriate tools to research Internet content.
    - The evaluation of online materials is a part of teaching and learning and will be undertaken regularly by tutors.
    - If staff or learners discover unsuitable sites, the URL (address) and content must be reported to the Head of College.
- **MANAGING INFORMATION SYSTEMS**
    - The security of the college information system and users will be reviewed regularly.
    - Virus protection will be updated regularly.
    - Unapproved software will not be allowed in work areas or attached to email.
    - Files held on the college's systems will be checked.
    - The use of user logins and passwords to access the college systems will be enforced.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Grow 19 will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Learners will be appropriately supervised when using technology, according to their ability and understanding.

7.2 Filtering and Monitoring

Configurable web content filtering covers usage on all College devices and learner mobile telephones when used within the Grow 19 premises at The East Malling Centre and whilst connected to the Grow 19 network.

7.2.1 Filtering

- Broadband connectivity is provided through Daisy. Staff and learners also have access to broadband through The East Malling Centre's Broad band provider.
- Grow 19 uses Fortinet Firewall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- If learners discover unsuitable sites, they will be required to:
    - Report the URL (address) and content to the Head of College
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL, who will action accordingly.
    - The Head of college will report to the IT Sytems Administrator.
    - The breach will be recorded and escalated as appropriate.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

7.2.2 Monitoring

Grow 19 will appropriately monitor internet use on all setting owned or provide internet enabled devices. This is achieved by physical monitoring (supervision) and monitoring internet and web access by reviewing logfile information. All users will be informed that use of

our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

If a concern is identified:

- All members of the college community will be informed about the procedure for reporting online safety concerns
- Record all incidents.
- Report to the DSL with concerns escalated appropriately following the normal procedures for raising concerns.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the college will contact the appropriate Safeguard Team or /and Education Safeguarding Advisor (Online Protection) and escalate the concern to the Police.

7.3.1 Decision Making

- Grow 19 Directors and senior leaders have ensured that our setting has appropriate filtering in place, to limit learner's exposure to online risks.
- Grow 19's decision regarding filtering and monitoring has been informed by a risk assessment, considering the specific needs, age and mental capacity of the learners.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience.
- The Head of College will ensure that regular checks are made to ensure that the filtering is effective and appropriate.
- All members of staff are aware that they cannot rely on filtering alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

7.5 Security and Management of Information Systems

- Grow 19 takes appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files
  - The appropriate use of user logins and passwords to access College devices and systems.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Passwords

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

- All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Change their passwords regularly.
    - Always keep their password private; users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

7.6 Managing the Safety of our Website

- Grow 19 will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- Grow 19 will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- Grow 19 will post appropriate information about safeguarding on our website for members of the community.

7.7 Publishing Images and Videos Online

- Grow 19 will ensure that all images and videos shared online are used in accordance with the learner agreement, acceptable use policy and social media and use of personal devices and mobile phones.

7.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted.

7.8.1 Staff email

- The use of personal email addresses by staff for any official school business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.
- Staff will only use official college provided email accounts to communicate with learners and parents/carers.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

7.8.2 Learner email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

7.9 Educational use of Videoconferencing and/or Webcams

- Grow 19 recognises that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
    - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
    - Videoconferencing contact details will not be posted publicly.
    - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Learner consent will be obtained prior to learners taking part in videoconferencing activities.
- Videoconferencing will be supervised appropriately, according to the learners ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- Grow 19 will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

7.10 Management of Learning Platforms

- Grow 19 does not currently use a Virtual Learning Platform, section 7.10 will be reviewed in light of any changes regarding this when required.

7.11 Management of Applications (apps) used to Record Learners's Progress

- Grow 19 track learners progress and share appropriate information with parents and carers, with agreement of the learner.
- The Principal is ultimately responsible for the security of any data or images held of learners. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
    - Only learner or College devices will be used for apps that record and store learners' personal details, attainment or photographs.
    - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
    - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Grow 19.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Grow 19 are expected to engage in social media in a positive, safe and responsible manner.
    - All members of Grow 19 are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Grow 19 will monitor learner and staff access to social media whilst using school provided devices and systems on site.

    - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action
- Concerns regarding the online conduct of any member of Grow 19 on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, behaviour and safeguarding policies.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Grow 19 on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Head of College immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as ‘friends’ any current or past learners or their family members via any personal social media sites, applications or profiles.
    - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL and the Head of College.

    - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head of College.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL.

8.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via appropriate sites and resources.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and safeguarding.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's knowledge or presence.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

8.4 Official Use of Social Media

- Grow 19 official social media channels are:
    - Facebook Grow 19 - Home | Facebook
    - Twitter Grow 19 (@19Grow) / Twitter
    - Instagram Grow 19 (@19grow) • Instagram photos and videos
    - You tube Grow 19 - YouTube
    - Friends of Five Acre Wood and Grow 19 (fofawgrow19.org.uk)
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
    - The official use of social media as a communication tool has been formally risk assessed and approved by the Principal and Directors.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected and, where possible, run and linked to the college website.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

- Official social media use will be conducted in line with existing policies.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated.
    - Learners will give consent to use of their image or video
- Grow 19 will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign the social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the college.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Ensure that they have appropriate consent before sharing images on the official social media channel.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
    - Inform their line manager or the DSL of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Personal Devices and Mobile Phones

- Grow 19 recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

9.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and ‘smart’ watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and safeguarding.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

    - All members of Grow 19 are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of Grow 19 are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy and disciplinary process.
- All members of Grow 19 are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or safeguarding policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, safeguarding adults at risk, data security and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to ‘silent’ mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as ‘airdrop’) are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless written permission has been given by the Head of College, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
- Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment or the learner’s phone during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with the code of conduct/staff behaviour and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

    - If there is suspicion that material on a learner’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches our policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- College mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- College mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of Grow 19 will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of Grow 19 must respect confidentiality and the need to follow the official procedures for reporting concerns.
  - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- Grow 19 require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or/and Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our school (for example if other local schools are involved or the public may be at risk), the DSL or Head of College will speak with Kent Police and the Education Safeguarding Team first to ensure that potential investigations are not compromised.

10.1 Concerns about Learner Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns. They will be recorded and act upon information in line with our safeguarding policy and protocols.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent and Medway Safeguarding thresholds and procedures.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Head of College. As staff are seconded from Five Acre Wood School, The Head of College will contact the Headteacher at Five Acre Wood School, to be considered in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Learners

- Our setting has accessed and understood "Sexual violence and sexual harassment between learners in schools and colleges" (2018) guidance and part 5 of 'Keeping learners safe in education' 2022.
- Grow 19 recognises that sexual violence and sexual harassment between learners can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. The response to concerns relating to sexual violence and sexual harassment between learners would follow Safeguarding protocols detailed within the safeguarding adults at risk and anti-bullying policies.
- Grow 19 recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Grow 19 also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Grow 19 will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between learners by implementing a range of ability appropriate educational methods as part of our PSD curriculum.
- Grow 19 will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.
- Grow 19 will respond to concerns regarding online sexual violence and sexual harassment between learners, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, Grow 19 will:
    - Immediately notify the DSL and act in accordance with our safeguarding adults at risk and anti-bullying policies
    - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.

- If appropriate, make a referral to partner agencies, such as Learner's Social Work Service and/or the Police.
- If the concern involves learners and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSLwill discuss this with Kent Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

11.2 Youth Produced Sexual Imagery ("Sexting")

- Grow 19 recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL.
- Grow 19 will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCMP guidance: "Responding to youth produced sexual imagery".
- Grow 19 will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- Grow 19 will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- Grow 19 will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- Grow 19 will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
    - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, Grow 19 will:
  - Act in accordance with our Safeguarding policies and the relevant Adult Safeguarding procedures (KASAF).
  - Ensure the DSL responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any susceptibility of learners involved; including carrying out relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Learners's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
  - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.

- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a learner/child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- Grow 19 will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target learners and how to respond to concerns.
- Grow 19 recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.
- Grow 19 will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of ability appropriate education for learners, staff and parents/carers.
- Grow 19 will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- Grow 19 will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), Grow 19 will:
    - Act in accordance with child protection policies and Kent Children's Safeguarding procedures and the relevant Kent Adult Safeguarding procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Learner's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
    - Carry out a risk assessment which considers any susceptibilities of learner(s) involved (including carrying out relevant checks with other agencies).
    - Inform parents/carers, if appropriate, about the incident and how it is being managed.
    - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
    - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- Grow 19 will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/ or and www.fearless.org

- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If learners at other setting are believed to have been targeted, the DSL will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Learners (IIOC)

- Grow 19 will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Learners (IIOC).
- Grow 19 will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- Grow 19 will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, Grow 19 will:
    - Act in accordance with our Safeguarding policy and the relevant Kent Safeguarding procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of learners, Grow 19 will:
    - Ensure that the DSL is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of learners have been found on the setting provided devices, Grow 19 will:
    - Ensure that the DSL is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and Learner's Social Work Service (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of learners on setting provided devices, Grow 19 will:
    - Ensure that the Head of College is informed. As staff are seconded from Five Acre Wood School, The Head of College will contact the Headteacher at Five Acre Wood School, in accordance with the allegations policy

- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

11.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Grow 19.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Grow 19 and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of Grow 19 will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.7 Online Radicalisation and Extremism

- Grow 19 will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Safeguarding Adults at Risk policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Head of College and Headteacher of Five Acre Wood School will be informed immediately, and action will be taken in line with safeguarding and allegations policies.

12. Useful Links for Educational Settings

Kent Support and Guidance for Educational Settings

Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, Online Safety Development Officer
  - Tel: 03000 415797
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-learners-and-young-people/child-protection-and-safeguarding
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
  - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
  - Kent Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP:

www.kscmp.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eiskent.co.uk

National Links and Resources

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Prevent www.ltai.info/what-is-prevent

National Links and Resources for Learners /Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- www.fearless.org