The Granville School

Online Safety Policy

Key Details

Designated Safeguarding Lead: Louise Lawrance Headmistress

Designated Safeguarding Deputy: Louise McCabe-Arnold Deputy Headmistress

Named Governor with lead responsibility: Mr Dougal Philps

Date written: September 2019

Date agreed and ratified by Governing Body:

Date of next review: September 2020

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

Contents

The Granville School Online Safety Policy

Policy aims

- **This online safety policy has been written by The Granville School 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' 2019, Early Years and Foundation Stage 2017 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of The Granville School online safety policy is to
    - safeguard and promote the welfare of all members of The Granville School community online.
    - identify approaches to educate and raise awareness of online safety throughout our 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 follow when responding to online safety concerns.

- The Granville School 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.

Policy scope

- The Granville School recognises 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.
- The Granville School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles are an important part of everyday life which present positive and exciting opportunities, as well as challenges and risks.
- The Granville School will empower our learners to acquire the knowledge needed to use the internet and technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.
- 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 and parents and carers.

- This policy applies to all access to the internet and use of technology, including mobile technology, or where learners, staff or other individuals have been provided with setting issued devices for use, both on and off-site.

Links with other policies and practices

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
    - Behaviour and discipline policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security
    - Cameras and image use policy
    - Searching, screening and confiscation policy

Monitoring and review

- Technology evolves and changes rapidly; as such The Granville School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local child protection concerns and/or any changes to our technical infrastructure.
- We 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 headmistress will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.
- Any issues identified via monitoring policy compliance will be incorporated into our action planning.

Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Louise Lawrance, Headmistress is recognised as holding overall lead responsibility for online safety.
- The Granville School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of The Granville School life.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Work with technical staff (CTS) and IT Department to ensure that suitable and appropriate filtering and monitoring systems are in place.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access regarding online safety concerns.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensure that staff, learners and parents/carers are proactively engaged in activities which promote online safety.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum which enables all learners to develop an appropriate understanding of online safety.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact within the setting on all online safeguarding issues.
- Liaise with other members of staff, such as pastoral support staff, IT technicians and Head of Computing on matters of online safety.
- Ensure appropriate referrals are made to relevant external partner agencies, as appropriate.
- Work alongside deputy DSL to ensure online safety is recognised as part of the settings safeguarding responsibilities, and that a coordinated whole The Granville School approach is implemented.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge 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.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- 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 coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.

- Ensure that online safety is promoted to parents, carers and the wider community through a variety of channels and approaches.
- 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 and The Granville School policies and procedures.
- Report online safety concerns, as appropriate, to The Granville School senior management team and Governing Body.
- Work with the Head of Computing teacher to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding *and/or* online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of our online safety policies.
- Read and adhere to our online safety policy and acceptable use of technology policies.
- Take responsibility for the security of IT systems and the electronic data they use or have access to.
- Model good practice when using technology with learners
- 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 the learners in their care.
- Identify online safety concerns and take appropriate action by following The Granville School safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting learners and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

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

- Provide technical support and perspective to the DSL and The Granville School leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures including *(including access control, password policies and encryption)* as directed by the leadership team to ensure that the settings IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy and monitoring systems and approaches are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL and/or deputies to enable them to take appropriate safeguarding action when required.

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

- Engage in age/ability appropriate online safety education.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, on and offline.
- Take an appropriate level of responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

It is the responsibility of parents and carers to:

- Read our acceptable use of technology policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the acceptable use of technology policies.
- Seek help and support from The Granville School or other appropriate agencies, if they or their child encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as SchoolBase and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their children access and use at home.

Education and engagement approaches

Education and engagement with learners

- The setting will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
    - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - implementing appropriate peer education approaches through the Student Council.
    - creating a safe environment in which all learners feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.

  - involving the DSL (or a deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any learners who may be impacted by the content.
  - making informed decisions to ensure that any educational resources used are appropriate for our learners.
  - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
  - providing online safety education as part of the transition programme across the key stages and/or when moving between establishments.
  - rewarding positive use of technology by pupils.

- The Granville School will support learners to understand and follow our acceptable use policies in a way which suits their age and ability by:
  - displaying acceptable use posters in all rooms with internet access.
  - informing learners that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
  - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- The Granville School will ensure learners develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
  - ensuring age appropriate education regarding safe and responsible use precedes internet access.
  - teaching learners to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Vulnerable Learners

- The Granville School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on their age, developmental stage and personal circumstances. However, there are some learners, for example looked after children and those with special educational needs, who may be more susceptible or may have less support in staying safe online.
- The Granville School will ensure that differentiated and appropriate online safety education, access and support is provided to vulnerable learners.

- Staff at The Granville School will seek input from specialist staff as appropriate, including the DSL and Learning Development Staff to ensure that the policy and curriculum is appropriate to our community's needs.

Training and engagement with staff

- We 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 training for all staff on a regular basis, with at least annual updates, which is integrated, aligned and considered as part of our overarching safeguarding approach.
    - Staff training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
    - build on existing expertise by provide opportunities for staff to contribute to and shape our online safety approaches, including curriculum, 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, including personal use of social media, can have an impact on their professional role and reputation.
    - highlight useful educational resources and tools which staff could use with learners.
    - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

- The Granville School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by
    - providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training.
    - drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and on SchoolBase) as well as in our prospectus and on our website.
    - requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
    - requiring them to read our acceptable use policies and discuss the implications with their children.

Reducing Online Risks

- The Granville School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We 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 their use in school is permitted.
    - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that access is appropriate.
    - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems or devices and as such identify clear procedures to follow if breaches or concerns arise.
- 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. This is clearly outlined in our acceptable use of technology policies and highlighted through a variety of education and training approaches.

Safer Use of Technology

Classroom use

- The Granville School uses a wide range of technology. This includes access to
    - Computers, laptops, tablets and other digital devices
    - Internet, which may include search engines and educational websites
    - SchoolBase/intranet
    - Email
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use of technology policies and with appropriate safety and security measures in place.
- iPads are only used with a teacher present.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use appropriate search tools as identified following an informed risk assessment.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of internet access and technology use will be appropriate to learners age and ability.
    - **Early Years Foundation Stage and Juniors**

        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - **Senior School**
        - Learners will use age-appropriate search engines and online tools.
        - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing internet access

- We will maintain a record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and agree an acceptable use policy before being given access to our computer system, IT resources or the internet.

Filtering and monitoring

Decision making

- The Granville School governors and IT Department have ensured that our school has age and ability appropriate filtering and monitoring in place to limit learner's exposure to online risks.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- The governors and leaders are mindful to ensure that "over blocking" does not unreasonably restrict access to educational activities and safeguarding materials.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Appropriate filtering

- The Granville School's education broadband connectivity is provided through EIS, who are owned by KCC. We work with EIS to ensure that our filtering policy is continually reviewed.
- The Granville School uses LightSpeed
    - LightSpeed blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft,

pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
    - LightSpeed is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
    - LightSpeed integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'
- We work with EIS to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.
- If learners or staff discover unsuitable sites or material, they are required to report the concern immediately to a member of staff who will then report the URL of the site to Head of Computing.
- Filtering breaches will be reported to the DSL (or deputy) and technical staff and will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving learners.
- Any access to material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, the police and/or CEOP.

Appropriate monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
    - physical monitoring (supervision),
    - monitoring internet and web access (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 via monitoring approaches the DSL or deputy will respond in line with the child protection policy.

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.
    - Full information can be found in our data protection policy which can be requested from the school office

Security and management of information systems

- We take 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.
- Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
- Checking files held on our network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for all users
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

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

- From year 3 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.
    - not share passwords or login information with others or leave passwords/login details where others can find them.
    - not to login as another user at any time.
    - lock access to devices/systems when not in use.

Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We 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.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies.

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 of technology 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 to set up personal social media accounts.
- Members of the community will immediately tell the headmistress 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; access to external personal email accounts may be blocked on site.

Staff email

- All members of staff are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- 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.

Learner email

- Learners will use a provided email account for educational purposes.
- Learners will agree an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses will be used for communication outside of the setting.

Educational use of videoconferencing and/or webcams

- The Granville School recognise 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.

- Staff will ensure that external videoconferencing opportunities and 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.

Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- 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.

Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written 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.
- We 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.

Management of learning platforms

- The Granville School uses SchoolBase (adults) and PurpleMash (pupils) as its official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator.

    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of leadership before reinstatement.
    - A learner's parents/carers may be informed.
    - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership as part of an agreed focus or a limited time slot.

Management of applications (apps) used to record children's progress

- We use SchoolBase to track learners progress and share appropriate information with parents and carers.
- The headmistress will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data
    - only learner issued 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.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

Social Media

Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Granville School community.
- 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 The Granville School community are expected to engage in social media in a positive and responsible manner.
    - All members of The Granville School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using school's *provided* devices and systems on site.

    - The use of social media during school hours for personal use is not permitted for staff.
    - The use of social media during hours for personal use is not permitted for learners.
    - Inappropriate or excessive use of social media during school *hours* or whilst using school devices may result in removal of internet access and/or disciplinary or legal action.
- Concerns regarding the online conduct of any member of The Granville School community on social media, will be reported to the DSL and be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff personal use of social media

- The safe and responsible use of social media 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 and/or acceptable use of technology 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 school.
    - 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 services. 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 appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the setting.
- Members of staff are encouraged not to identify themselves as employees of The Granville School on their personal social networking accounts; this is to prevent information 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. Staff are expected 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 leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents/carers

- Staff will not use personal social media accounts to contact learners or parents/carers, nor should any contact be accepted.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions which compromise this requirement will be discussed with the DSL.
    - Decisions made and advice provided in these situations will be formally recorded in order to safeguard learners, the setting and members of staff.
- 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.
    - Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy

Learners 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 age appropriate sites and resources.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.
- Learners will be advised:
    - to consider the benefits and risks of sharing personal details or information 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 appropriate adults' permission, and to only do so when a trusted adult is present.
    - 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 on social media, both within the setting and externally.

Official use of social media

- At this moment in time, The Granville School does not have any official social media channels.

The following will apply if and when The Granville School does have official social media channels:

- The official use of social media sites by The Granville School will only take place with clear educational or community engagement objectives and with specific intended outcomes.
    - The official use of social media as a communication tool will have been formally risk assessed and approved by the headmistress and Senior leadership team.
    - Leadership staff will 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 will be set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff will use setting provided email addresses to register for and manage official social media channels.
    - Official social media sites will be suitably protected and, where possible, linked from our 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 will be will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny.
- Parents/carers and 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.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We 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 our social media acceptable use policy.
    - Be aware they are an ambassador for the setting.
    - Be professional, 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 appropriate consent has been given 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 private/direct messaging with current or past learners or parents/carers.
- Inform their line manager, the DSL (or deputy) of any concerns, such as criticism, inappropriate content or contact from learners.

Mobile Technology: Use of Personal Devices and Mobile

- The Granville School recognises that personal communication through mobile technologies is part of everyday life for many learners, staff and parents/carers. Mobile technology needs to be used safely and appropriately within the setting.

Expectations

- All use of mobile technology including mobile phones and personal devices such as tablets, games consoles and wearable technology will take place in accordance with our policies, such as anti-bullying, behaviour and child protection and with the law.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of The Granville School community are advised to take steps to protect their mobile phones or personal 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 The Granville School community 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 changing rooms, toilets and swimming pools.
- 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 in line with our anti-bullying and behaviour policies.
- All members of The Granville School community 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 child protection policies.

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, child protection, data security and acceptable use of technology.

- Staff will be advised to
    - keep mobile phones and personal devices in a safe and secure place (e.g. deskdrawer) 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 headmistress 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.
    - Any pre-existing relationships which could undermine this, will be discussed with the DSL (or deputy.
- Staff will not use personal devices or mobile phones:
    - 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 during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our 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 using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

Learners use of personal devices and mobile phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
    - The Granville School expects learners' mobile phones to be handed into the office for safekeeping during the school day.
- If a learner needs to contact his/her parents or carers they will be allowed to use school phone.
    - Parents are advised to contact their child via the school office
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
    - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.

    - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- If a learner breaches the policy, the phone or device will be confiscated and held in a secure place.
    - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our child protection, behaviour or anti-bullying policy.
    - Searches of mobile phone or personal devices will be carried out in accordance with our policy.
    - Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - Mobile phones and devices that have been confiscated will be released to parents/ carers.
    - 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.

Visitors' use of personal devices and mobile phones

- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and inform the DSL (or deputy) of any breaches of our policy.

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.
- The Granville School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- The Granville School mobile phones and devices will always be used in accordance with the acceptable use of technology policy and other relevant policies.

Responding to Online Safety Incidents

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, peer on peer abuse, including cyberbullying and youth produced sexual imagery (sexting), online sexual violence and harassment, online abuse and exploitation and illegal content.
- All members of the community will 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.
- We require staff, parents, carers and learners to work in partnership with us to resolve online safety issues.
- After any investigations are completed, leadership staff 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 (or deputy) will seek advice from the Education Safeguarding Service.
- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm as appropriate.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the DSL will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

Concerns about learner online behaviour and/or welfare

- The DSL (or deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
- All concerns about learners will be recorded in line with our child protection policy.
- The Granville School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online peer on peer abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to learners as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the headmistress, in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our *Capability, personnel and Grievance Policy*.
- Welfare support will be offered to staff as appropriate.

Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the DSL (or deputy). The DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

Procedures for Responding to Specific Online Concerns

Online sexual violence and sexual harassment between children

- Our DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2019.
    - Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
- The Granville School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;
    - Non-consensual sharing of sexual images and videos
    - Sexualised online bullying
    - Online coercion and threats
    - 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence
    - Unwanted sexual comments and messages on social media
    - Online sexual exploitation
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
    - immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - if content is contained on learners personal 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 implementing safety plans, offering advice on blocking, reporting and removing online content, and 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 referrals to partner agencies, such as Children's Social Work Service and/or the police.
    - if the concern involves children and young people at a different educational setting, the DSL will 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 DSL (or deputy) will discuss this with the 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.
- The Granville School 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.
- The Granville School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, The Granville School 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 by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

Youth produced sexual imagery ("sexting")

- The Granville School recognises youth produced sexual imagery (also known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and the local KSCMP guidance: "Responding to youth produced sexual imagery".
    - Youth produced sexual imagery or 'sexting' is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
    - It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
- The Granville School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing youth produced sexual imagery by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding the taking and sharing of youth produced sexual imagery. Advice to parents and staff can be found on our *website, intranet, staff room.*

- We 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.
- We will not:
    - view any suspected youth produced sexual imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so.
        - If it is deemed necessary, the imagery will only be viewed where possible by the DSL, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video 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, we will:
    - act in accordance with our child protection policies and the relevant local procedures.
    - ensure the DSL (or deputy) responds in line with the UKCIS and KSCMP guidance.
    - Store any devices containing potential youth produced sexual imagery securely
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially 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 in line with the UKCIS and KSCMP guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - make a referral to Children's Social Work Service and/or the police, as deemed appropriate in line with the UKCIS and KSCMP 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 UKCIS 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 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.

Online abuse and exploitation (including child sexual abuse and sexual or criminal exploitation)

- The Granville School recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL (or deputy), in line with our child protection policy.

- The Granville School will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target learners, and understand how to respond to concerns.
- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for learners, staff and parents/carers. The pupils learn about in in PSHCE and ICT lessons, Staff attend courses, INSET, updates and can access information via our safeguarding policy and website. Parents can also access information and advice via the school's website.
- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.
- We will ensure that the 'Click CEOP' report button used to report online child sexual abuse is visible and available to learners and other members of our community, which can be accessed via the internet and our Safeguarding policy.
- If made aware of an incident involving online child abuse and/or exploitation, we will:
    - act in accordance with our child protection policies and the relevant KSCMP procedures.
    - store any devices containing evidence securely.
        - If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
    - if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a learner is at immediate risk.
    - carry out a risk assessment which considers any vulnerabilities of learner(s) involved, including carrying out relevant checks with other agencies.
    - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
    - 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.
- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using setting provided or personal equipment.
    - Where possible and appropriate, learners will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via CEOP: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or 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 police by the DSL (or deputy).

- If members of the public or learners at other settings are believed to have been targeted, the DSL (or deputy) will seek advice from the police and/or the Education Safeguarding Service before sharing specific information to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- The Granville School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate to the age and ability.
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) 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 (or deputy) will obtain advice immediately through the police and/or the Education Safeguarding Service.
- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant KSCMP procedures.
    - store any devices involved securely.
    - immediately inform appropriate organisations, such as the IWF and police.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF 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 children have been found on the setting provided devices, we will:
    - ensure that the DSL (or deputy) is informed.
    - ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and Children'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) following a written request from the police.
    - report concerns, as appropriate to parents/carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
    - ensure that the headmistress is informed in line with our managing allegations against staff policy.
    - inform the Local LADO and other relevant organisations in accordance with our managing allegations against staff policy.

- quarantine any devices until police advice has been sought.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Granville
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy, which can be found on the school website.

Online hate

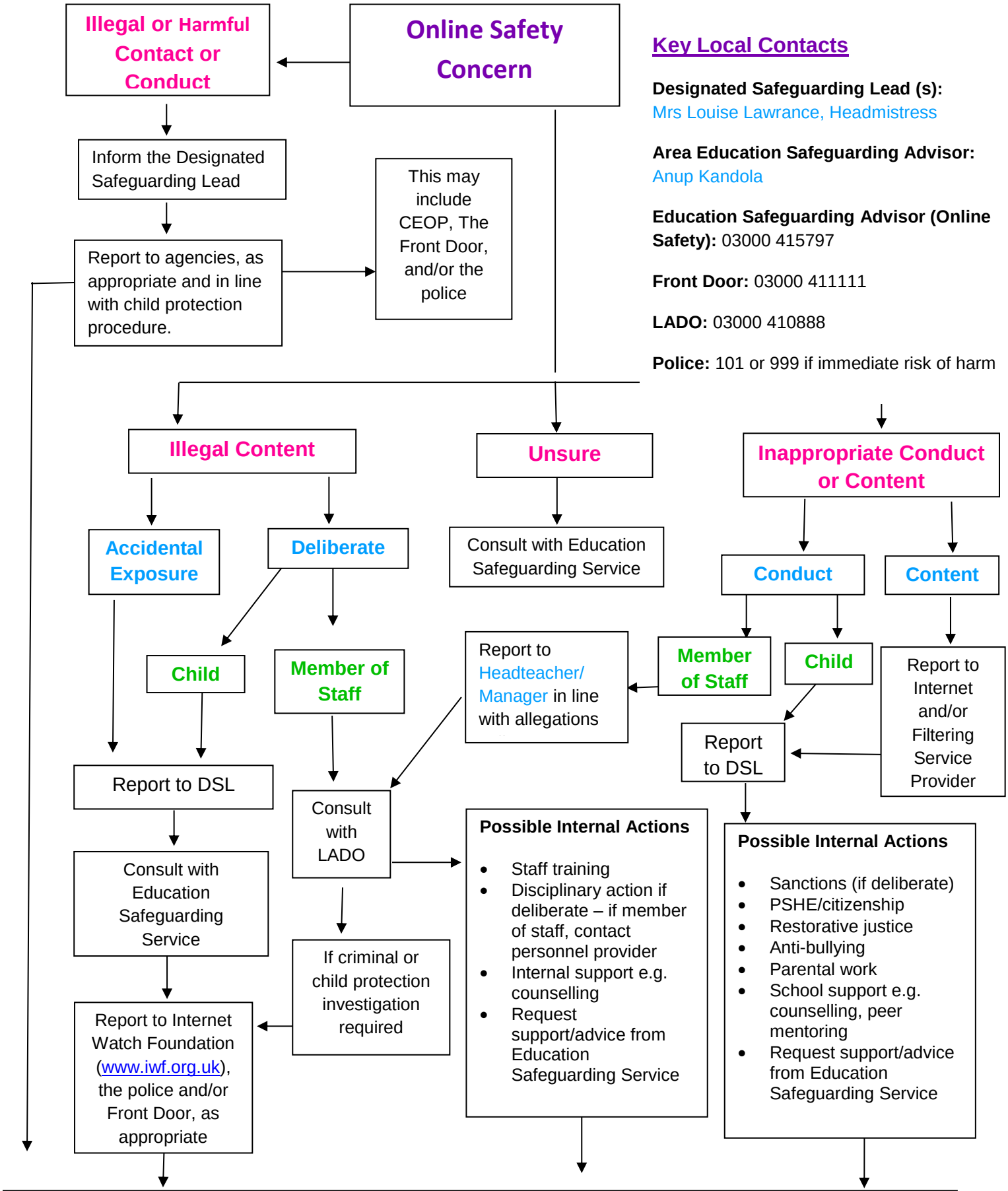
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at The Granville School and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.
- All members of the community will be advised to report 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 (or deputy) will obtain advice through the Education Safeguarding Service and/or the police.

Online radicalisation and extremism

- As listed in this policy, we 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 learner or adult may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.

If we are concerned that member of staff may be at risk of radicalisation online, the headmistress will be informed immediately, and action will be taken in line with the child protect and allegations policies

Responding to an Online Safety Concern Flowchart



Key Local Contacts

Designated Safeguarding Lead (s):
Mrs Louise Lawrance, Headmistress

Area Education Safeguarding Advisor:
Anup Kandola

Education Safeguarding Advisor (Online Safety): 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Police: 101 or 999 if immediate risk of harm

Written September 2109
Next review Sept 2020

Useful Links

Kent Educational Setting Support and Guidance

Education Safeguarding Service, The Education People:

- 03000 415797
    - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
    - Ashley Assiter, Online Safety Development Officer
- Guidance for Educational Settings:
    - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
    - www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCMP: www.kscb.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 non-urgent enquiries, contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk**:** www.eisit.uk

National Links and Resources for Settings, Learners and Parents/carers

- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk

- Internet Watch Foundation (IWF): www.iwf.org.uk

- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety

- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

  - Report Harmful Content: https://reportharmfulcontent.com/

- 360 Safe Self-Review tool for schools: www.360safe.org.uk

- Childnet: www.childnet.com
  - Step Up Speak Up – Online Sexual Harassment Guidance: www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals
  - Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

- Internet Matters: www.internetmatters.org

- Parent Zone: https://parentzone.org.uk

- Parent Info: https://parentinfo.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk

- Lucy Faithfull Foundation: www.lucyfaithfull.org

- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

- Action Fraud: www.actionfraud.police.uk

- Get Safe Online: www.getsafeonline.org

Appendix A: Acceptable Usage Policy: Staff

This document has been written to ensure that staff use the computers, personal electronic devises and mobile phones throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Management team or the computer department. Staff should:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines.
- Ensure that they have a sensible password.
- Ensure that usernames and passwords are not shared with children.
- Ensure that they log off when they have finished using a computer or lock the computer when they leave the room but are coming back e.g. break times.
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files on return too.
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper.
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times.
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum.
- Ensure that they are not using the school's computers for financial gain e.g. auction or betting sites.
- Ensure that they are not using the school's computers for social media sites.
- Ensure that they have read and understood the Computer Policy.
- Be aware that software or hardware should not be installed without prior consent of the computing department or Headmistress.
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Headmistress.
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Report any issues to the Headmistress or ICT department as soon as possible.
- Return any hardware or equipment if they are no longer employed by the school.
- Not use personal cameras or phones to take photographs of children within school, there are a number of school cameras available for everyday usage, trips and matches. Ensure mobile phones should be stored away from the children.

Signed _____

Print _____ Date _____ _____

Appendix B: Acceptable Usage Policy: KS2 Children

This document is to provide some guidelines to ensure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, iPads and everything else including cameras and other devices. By using the ICT in school, you have agreed to follow these rules. These rules will be discussed with you as a class before you sign them. A copy of this will also be sent home to your parents.

If you have any questions, please ask your teacher or Miss Barrow

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- When communicating online (in blogs, email etc) I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not logon using another person's account without their permission.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will take care when using the computers and transporting equipment around.
- I will keep my online usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers.
- I will not install any software or hardware (including memory sticks) without permission from a teacher.
- I understand that if I am acting inappropriately then my parents may be informed.

Signed (Pupil) _____ Class _____ Date _____

Signed (Parent) _____ Date _____

Appendix C: Acceptable Usage Policy: KS1 Children

These rules have been written to make sure that you stay safe when using the computers. This includes cameras and microphones too. By using the computers and iPads in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher or Miss Barrow.

The Golden Rule: **Think before you click**

We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

I will tell a teacher if I see something that upsets me.

Signed (Pupil) _____ Class _____ Date _____

Signed (Parent) _____ Date _____

Appendix D e-Reader Acceptable Use Policy and Agreement Form

eReaders are devices with E Ink screens, designed primarily for viewing books. Some examples include the Kindle, Nook and Sony Reader. The Granville School recognises that eReaders can provide a number of benefits for students, including the lightening of their bags, adjustable text sizes and colours, and access to thousands of free books.

The Granville School acknowledges that some eReaders can connect to the Internet through mobile connections (3G) that the school cannot control. Students therefore must not connect these devices to the Internet while at school.

Parents must sign a release stating that they are solely responsible for the content on their child's eReader. The nature of these devices makes it very difficult for teachers to monitor what students are reading, which is why we are insisting that parents be responsible for the use and content on their children's devices. If you choose to buy an eReader for your child to use in school, please take the time to become familiar with its operation so that you can regularly monitor what your child is reading.

Student Responsibilities and Permission

- I will not give my eReader (e.g. Kindle) to another student for his/her use
- I will not use my eReader for any purpose other than displaying reading material.
- I will not download, purchase, or change the content loaded on my eReader at school and without the permission of my parents

_____ _____ _____

Student name Student signature Date

Parent/Guardian Section:

I authorise my child to bring their e-Reader to The Granville School with the understanding that it is to be used as a tool for reading only and that my child will comply with the aforementioned eReader Acceptable Use Policy. I understand that The Granville School is not responsible for any damage or loss associated with my child's e-Reader. I also understand that a violation of the eReader policy may result in my child losing the privilege to bring their eReader to school for a length of time commensurate with the nature of the violation.

_____ _____ _____

Parent/Guardian name Parent/Guardian signature Date

Appendix E: Wi-Fi Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all members of The Granville School community are fully aware of the school's boundaries and requirements when using The Granville School Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of The Granville School community are reminded that technology use should be consistent with our ethos, other appropriate policies and the law.

1. The Granville School provides Wi-Fi for the school community and allows access for educational use only.

2. I am aware that The Granville School will not be liable for any damages or claims of any kind arising from the use of the wireless service. The Granville School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within school's premises that is not the property of The Granville School.

3. The use of technology falls under The Granville School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy and Safeguarding policy which all learners/staff/visitors and volunteers must agree to and comply with.

4. The Granville School reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. The Granville School owned information systems, including Wi-Fi, must be used lawfully; 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.

6. I will take all practical steps necessary to make sure that any equipment connected to The Granville School service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The Granville School wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of The Granville School wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The Granville School accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless The Granville School from any such damage.

9. The Granville School accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of The Granville School security and filtering systems or download any unauthorised software or applications.

12. My use of The Granville School Wi-Fi will be safe and responsible and will always be in accordance with the school's AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring The Granville School into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead (Headmistress) as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Headmistress)

16. I understand that my use of The Granville School Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If The Granville School suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then The Granville School may terminate or restrict usage. If The Granville School suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agreed to comply with The Granville School Wi-Fi acceptable Use Policy.

Name ……..

Signed: ……..Date (DDMMYY)……

Acknowledgements and Thanks

This document and statements have been produced by The Education People Education Safeguarding Service with thanks to members of Kent Education Online Safety Strategy Group.

Additional thanks to the UK Safer Internet Centre, South West Grid for Learning, Childnet , CEOP, The Judd School, Kingsnorth Primary School, Loose Primary School, Peter Banbury, Kent Police, Kent Schools Personnel Service (SPS), Kent Legal Services and Kent Libraries and Archives, for providing comments, feedback and support on previous versions.

Linked Policies:

- Anti-bullying policy
- Acceptable Use Policies (AUP)
- Code of conduct for staff
- Promotion of Good Behaviour Policy
- Safeguarding policy
- Computing and ICT
- Personal Social and Health Education (PSHE)
- Data Protection Policy
- CCTV policy