BORDEN GRAMMAR SCHOOL
Online (E-Safety) Policy

Date Drawn up	**October 2010**
Drawn up by	**Michelle Brooker based on The Education People Child Protection policy template and Mobile Technology & Social Media Policy September 2020**
Revised by	**Michelle Brooker**
Date Revised	**January 2021**
Date Ratified by Trustees (Standards)	**January 2021**
School E-Safety Co-Ordinator (and Designated Safeguarding Lead)	**Michelle Brooker**
School E-Safety Link Trustee	**Vicki Meacham**
Frequency of Review	**Annually**
Review Date	**January 2022**

Online (E-Safety) Policy
Contents Page

1.0 Creating an Online Safety Ethos

1.1. Aims and Policy Scope

1.1.1. This online safety policy has been written by Borden Grammar School, involving staff, pupils and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.

1.1.2 It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2020, 'Working Together to Safeguard Children' 2018 and the Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures, as well as updates from the DfE 'Safeguarding and Remote Education during Coronavirus (COVID-19) guidance'.

1.1.3 Borden Grammar School recognises that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to online risks and build resilience.

1.1.4 It is recognised by Borden Grammar School that the use of technology presents challenges and risks to children and adults both inside and outside of school. Borden Grammar School will empower, protect and educate the community in their use of technology and establish mechanisms to identify, intervene in, and escalate any incident where appropriate.

Borden Grammar School is currently operating in response to Coronavirus (COVID-19); our safeguarding principles in accordance with 'Keeping Children Safe in Education' (KCSiE 2020) and related guidance, however remain the same. Where children are asked to learn online at home in response to a full or partial closure, Borden Grammar School will follow expectations as set out within the Child Protection Policy, the Acceptable Use Policy and Addendums, and in line with DfE Guidance, 'Safeguarding and Remote Education during Coronavirus (Covid-19)' 2020.

1.1.5 Borden Grammar School identifies that the breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

1.1.6 Borden Grammar School 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.

1.1.7 Borden Grammar School identifies that the internet and associated devices, such as computers, tablets, mobile phones, games consoles and smart watches are part of everyday life for all students and staff.

1.1.8 This policy applies to all staff including the Board of Trustees, leadership team, teachers, support staff, external staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

1.1.10 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 school issued devices for use off-site, such as a work laptop or mobile phone.

1.1.11 This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social Health and Education (PSHE), Citizenship and Relationships and Sex Education (RSE) and Staff Code of Conduct.

1.1.12 The policy will be monitored in the following manner:

The E-Safety policy was approved by the Board of Trustees' Personnel & Pastoral Sub-Committee:	January 2021
The implementation of the E-Safety policy will be monitored by an E-Safety Group:	Michelle Brooker (AHT & DSL) Richard Artingstoll (AHT & DSL trained) Angela Bryant (HoD ICT) Julian Pilford-Bagwell (Network Manager) Vicki Meacham (School E-Safety Link Trustee)
The E-Safety Group will meet:	Annually
The E-Safety Group will present an anonymised report:	Annually to the Board of Trustees Personnel & Pastoral Sub-Committee.
Monitoring of filtering and control logs	Network Manager (termly)
Logs of Reported Incidents monitored by Designated Safeguarding Lead	Michelle Brooker (termly)
E-Safety Staff Training Updates	Michelle Brooker & Richard Artingstoll (annually)

1.2 Writing and Reviewing the Online Safety Policy

- Borden Grammar School's online safety policy has been written by the school, building on the KCC online safety policy template with specialist advice and input as required.
- It takes into account the DfE statutory guidance "Keeping Children Safe in Education" 2020 and the Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures.
- The school's policy has been approved and agreed by the Senior Leadership Team and the Board of Trustees.
- The School has appointed a member of the Board of Trustees to take lead responsibility for online safety (e-Safety).
- The school has appointed a member of the leadership team as the online safety lead, the Designated Safeguard Lead.
- The school's online safety (e–Safety) Policy and its implementation will be reviewed at least annually or sooner if required.

1.3.1 Key Responsibilities of the School Community

- All members of Borden Grammar School community have an essential role to play in ensuring the safety and wellbeing of others, both on and offline. It is important that all members of the community are aware of these roles and responsibilities and also how to access and seek support and guidance. This policy enables staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology. It identifies clear procedures to use when responding to online safety concerns.

Key responsibilities of the senior leadership team are:

- 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 Code of Conduct and an AUP, which covers acceptable use of technology.
- Ensure that there are suitable and appropriate filtering and monitoring systems in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive whole curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead and Deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the school 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
- If appropriate, 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 People's Education Safeguarding service, or other agency in accordance with our Child Protection policy.

1.3.2. Key responsibilities of The Designated Safeguarding Lead (DSL):

- Act as a named point of contact on all online safety issues and liaise with other members of staff or other agencies as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Keeping up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training, e.g. Prevent Online Training.
- Access regular and appropriate training and support to ensure they recognize the additional risks that learners with SEN&D face online.
- 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 schools 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 management team and Board of Trustees.
- Work with the senior leadership team to review and update online safety policies on a regular basis (at least annually).
- Meet annually with the trustee with a lead responsibility for safeguarding and/or online safety.

1.3.3. The key responsibilities for **all members of staff** are:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- Take responsibility for the security of school 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 the children in their care.
- Identify online safety concerns and take appropriate action by following

the school's 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.

1.3.4. **It is the responsibility of staff managing the technical environment to**:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures (including password policies and encryption) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure appropriate access and technical support is given to the DSL and deputies regarding the filtering and monitoring systems, to enable them to take appropriate safeguarding action as required.

1.3.5. The key responsibilities of **pupils** are:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school acceptable use policies.
- 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.

1.3.6. The key responsibilities of **parents and carers** are:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school's online safety policy
- Use school 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.

2.0 Education and Engagement Approaches

2.1 Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum, to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in the PD and ICT programmes of study.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

The school will support pupils to read and understand the AUP in a way which suits their age and ability by:

- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Using support, such as external visitors, where appropriate, to complement and support the school's internal online safety education approaches.
- The school will question students during Deep Dive student voice interviews on e-safety

2.1.1 Vulnerable Pupils

- Borden Grammar School is aware that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Borden Grammar School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- Borden Grammar School will seek input from specialist staff as appropriate, including the SENCO.

2.1.2 Training and engagement with staff

The school will:

- Ensure that online safety training for all staff is integrated, aligned and considered as part of our overarching safeguarding approach.
- Provide and discuss the online safety policy 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 (as part of annual safeguarding training/updates or within separate or specific online safety sessions or updates).
- This will cover the potential risks posed to pupils (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 school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, 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 pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

2.1.3 Awareness and engagement with parents and carers

- Borden Grammar School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.

The school 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 via Parent Mail and the school website. This will include offering online safety awareness at events such as parent evenings, transition evenings.
- Drawing their attention to the school online safety policy and expectations in parent mail, letters and on our website.
- Requesting that they read online safety information as part of joining our school.
- Requiring them to read the school's acceptable use policies and discuss the implications with their children.

3.0 Reducing Online Risks

- Borden Grammar 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 use in school is

permitted.
    - Ensure that appropriate filtering and monitoring 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 a school computer or device, e.g. smartwatches.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting or forwarding any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's Acceptable Use Policy and highlighted through a variety of education and training approaches.

4.0 Safer Use of Technology

4.1.1 Classroom Use

- Borden Grammar School 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
- School learning platform (Moodle) /intranet, Google Suite
- Email
- Digital cameras and video cameras
- All school owned devices will be used in accordance with the school's Acceptable Use Policy and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of the school.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Learners will be directed to use age appropriate online resources and tools by staff.

Key Stage 3, 4, 5:

- Pupils will be appropriately supervised when using technology, according to their ability and understanding.

4.1.2 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an Acceptable Use Policy before being given access to the school computer system, IT resources or internet.

4.1.3 **Filtering and Monitoring**

4.1.4 **Decision Making**

- Borden Grammar School Trustees and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The Trustees and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's 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.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

4.1.5 **Filtering**

- Educational broadband connectivity through BT Internet
- The school uses Diladele Web Safety Filtering System which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The school filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- The school works with BT Internet and Diladele Web Safety Filtering System to ensure that our filtering policy is continually reviewed.
- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead (or Deputy) and/or technical staff.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

4.1.7 **Monitoring**

- The school will appropriately monitor internet use on all school owned or

provided internet enabled devices. This is achieved by:

- Physical monitoring (supervision), monitoring internet and web access (reviewing log in information) and active technology monitoring services.
- The school has a clear procedure for responding to concerns identified via monitoring approaches e.g. DSL will respond in line with the child protection policy
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

4.1.8 **Managing Personal Data Online**

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulation and the Data Protection Act 2018.

4.1.9 **Security and Management of Information Systems**

- The school 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)
- 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 held on the school's network,
- The appropriate use of user logins and passwords to access the school network.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found in the Acceptable Use Policy

Password policy

- All members of staff will have their own unique username and private password to access the school systems; members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access the schools systems; pupils are responsible for keeping their passwords private
- We require all users to:

  Use strong passwords for access into our system

  Always keep their password private; users must not share it with others or leave it where others can find it

  Not to login another user at any time.

4.1.10 **Managing the Safety of the School Website**

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school 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 pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

4.1.11 **Publishing Images and Videos Online**

- The school will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to): the Image use policy, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.

4.1.12 **Managing Email**

- Access to school email systems will always take place in accordance with data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Staff Code of conduct.
- 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.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell (the DSL) if they receive offensive communication, and this will be recorded in the school 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 in school.

4.1.13 **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 a specific school 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 and pupils and parents.

4.1.14 **Pupil email**

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

Where children are asked to learn online at home in response to a full or partial closure:

- Borden Grammar School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.
- All communication with learners and parents/carers will take place using school/college provided or approved communication channels; for example, school/college provided email accounts and phone numbers and/or agreed systems e.g. Google Classroom.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.
- Staff and learners will engage with remote teaching and learning in line with existing behaviour principles as set out in our Behaviour policy and Acceptable Use Policies.
- Staff and learners will be encouraged to report issues experienced at home and concerns will be responded to in line with our Child Protection and other relevant policies.
- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP).
- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Borden Grammar School will continue to be clear who from the school (if anyone) their child is going to be interacting with online.
- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.
-

4.1.15 **Educational use of Videoconferencing**

- Borden Grammar School recognises that videoconferencing can be a challenging activity but brings a wide range of learning benefits.
- All videoconferencing 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.
- School videoconferencing equipment will not be taken off school 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.

4.1.16 **Users**

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and 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.

4.1.17 **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.

4.1.18 **Management of Learning Platforms**

- Borden Grammar School uses Google as its official Learning Platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message/communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled.
- Pupils 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 considered to be illegal, then the school 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; in this instance, there may be an agreed focus or a limited time slot.

4.1.19 **Management of Applications (apps) used to Record Children's Progress**

- The school uses SIMS and Edulink to track pupils' progress and share appropriate information with parents and carers.
- The school uses 4Matrix to track GCSE and A Level pupil progress.
- The Headteacher is ultimately responsible for the security of any data or images held of children. 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 Regulation (GDPR) and the Data Protection Act 2018.

In order to safeguard pupils' data:

- Only school issued devices will be used for apps that record and store children's 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 children's personal details, attainment or images.
- School 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.

5.0 Social Media

5.1 Expectations

- The expectations regarding safe and responsible use of social media applies to all members of Borden Grammar 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 Borden Grammar School community are expected to engage in social media in a positive, safe and responsible manner. Safe and professional behaviour will be outlined for all members of staff

(including volunteers) as part of the school Code of Conduct within the Acceptable Use Policy.

- All members of Borden Grammar School community 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.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- The use of social media during school hours for personal use is not permitted.
- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Borden Grammar School community on social media, should be reported to the DSL and will be managed in accordance with our Acceptable Use, Anti-Bullying, Allegations against Staff, Behaviour and Child Protection policies.

5.2 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 the school code of conduct within the AUP.
- Any complaint about staff misuse or policy breaches will be referred to the Headteacher 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).
- If appropriate, disciplinary and/or legal action will be taken in accordance with our staff behavior policies/ code of conduct.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school.
- Legal or disciplinary action may be taken if they 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 as strictly as they can.
    - 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.
    - Keeping passwords safe and confidential.
    - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of Borden Grammar school on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also 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 with schools' 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 pupils 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 in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' 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 Designated Safeguarding Lead (or Deputy) and/or the Headteacher.
    - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead (or Deputy).

5.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. Further information is contained within our curriculum policies: IT, RSE
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies

including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

Pupils 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. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
- 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 permission and only when a trusted adult is present.
- To use safe strong 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 school and externally.

5.4 Official Use of Social Media

Borden Grammar School official social media channels are:

  - Twitter and Facebook

- The official use of social media sites, by the school, 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 Headteacher.
- Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence or school closure.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Staff use school provided email addresses to register for and manage any official school social media channels.
- Official social media sites are suitably protected and run from the school website.
- Public communications on behalf of the school 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, including: Anti-bullying, Image use, Data protection, Confidentiality and Child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Social media tools Facebook and Twitter have been risk assessed and approved as suitable for educational purposes.
- Parents and carers will be informed of any official social media use with pupils and 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 the school 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 school, they will:
- Sign the school's Acceptable Use Policy.
- Always be professional at all times and aware that they are an ambassador for the school.
- Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
- 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 school unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
- Inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

6.0 Use of Personal Devices and Mobile Phones

- Borden Grammar School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

6.1 Expectations

- All use of personal devices (including but not limited to; tablets, e-readers games consoles and wearable technology, such as smart watches and fitness trackers which facilitate communication or have the capability to record sound or imagery) and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited

to: anti-bullying, behaviour and child protection.

- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
    - All members of Borden Grammar School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
    - All members of Borden Grammar 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 and toilets.
- The sending of abusive or inappropriate messages/ 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 or Child protection policy.
- All members of Borden Grammar School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's Behaviour or Child Protection policies.

6.2 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 school policy and procedures, such as: Confidentiality, Child Protection, 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.
- 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 pupils or parents and carers, unless given prior approval from the Headteacher following a formal risk assessment. Staff will follow clear guidance outlined in the AUP.
- Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead or Deputy and/or Headteacher.
- If a member of staff breaches the school policy, action will be taken in line with the staff code of conduct 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, and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

6.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Borden Grammar School expects pupil's personal devices and mobile phones to be on silent and kept out of sight during lessons
- If a pupil needs to contact his/her parents or carers they will be allowed to use the office phone.
    - Parents are advised to contact their child via the school office during school hours.
- Mobile phones or personal devices will not be used by pupils during lessons 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.
- Where learners' mobile phones or personal devices are used when learning at home, such as in response to a local or full lockdown this will be in accordance with the AUP.
- Mobile phones and personal devices including but not limited to smartwatches and Fitbits if taken into examinations will be handed to the invigilators.
- Pupils found in possession of a mobile phone or personal device, including but not limited to smartwatches and Fitbits, during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in the school office until the end of the day.
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery or other illegal videos or images.
- Learners' mobile phones or devices may be searched by a member of the leadership team. Content may be deleted or requested to be deleted, if it contravenes our Acceptable Use or school behaviour policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be safely stored and handed over to the police for further investigation.

6.4 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 the school's Acceptable Use Policy and other associated policies, such as: Anti-bullying, Behaviour, Child Protection and Image Use.

- Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our Acceptable Use Policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead (or Deputy) of any breaches of school policy.

6.5 Officially provided mobile phones and devices.

- Members of staff will be issued with a work email address, where contact with pupils or parents/ carers is required.
- 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.
- School mobile phones and devices will always be used in accordance with the AUP.
- Where staff or learners are using Borden Grammar School provided devices, they will be informed prior to use, that activity may be monitored for safeguarding reasons and to ensure policy compliance.

7.0 Responding to Online Safety Incidents and Concerns

- All members of the school community 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 the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL (or Deputy) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or 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 the school community (for example if other local schools are involved or the public may be at risk), the DSL or Headteacher will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised. The DSL or Deputy will pass relevant information to other DSL's if appropriate.

7.1 Concerns about Pupils Welfare

- The DSL (or Deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or Deputy) will record these issues in line with the school's child protection policy.
- The DSL (or Deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Multiagency Partnership (KCSMP) thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

7.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, according to 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 Behaviour policy and staff Code of Conduct.

8.0 Procedures for Responding to Specific Online Incidents or Concerns

8.1.1. Online Sexual Violence and Sexual Harassment between Children

Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2019) guidance and part 5 of 'Keeping Children Safe in Education' 2020.

Borden Grammar 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, unwanted sexual comments and messages on social media, and online sexual exploitation.

Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.

Borden Grammar School recognises that the 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.

Borden Grammar School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

Borden Grammar 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 between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.

We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.

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 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' 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 Children's Social Work Service and/or the Police.
- If the concern involves children 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 DSL (or Deputy) will 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.

8.1.2 Youth Produced Sexual Imagery ('Sexting')

- Borden Grammar School recognises youth produced sexual imagery (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 UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- Borden Grammar School 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.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- 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 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 (or Deputy 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, we will:

- Act in accordance with our child protection policies and the relevant Education Safeguarding Service guidance.
- Ensure the DSL (or Deputy) 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 vulnerability 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 Children'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 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.

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

- Borden Grammar School 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 children and how to respond to concerns.
- Borden Grammar School 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 Designated Safeguarding Lead (or Deputy).
- The school will implement preventative approaches for online child sexual

abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.

- The school 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.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community. It can be accessed on the school website and Moodle.

8.1.4 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse and exploitation (including criminal exploitation), we will:
- Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Multiagency Partnership's procedures.
- Immediately notify the Designated Safeguarding Lead.
- If appropriate store any devices involved securely.
- Make a referral to Children'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 vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- We 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/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead (or Deputy) will obtain advice immediately through the Education Safeguarding Service and/or Kent Police.
- If the school is 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 Designated Safeguarding Lead (or Deputy).
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

8.2 Indecent Images of Children (IIOC)

- Borden Grammar School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will respond to concerns regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action 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 the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead (or Deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Service.

If made aware of IIOC, the school will:

- Act in accordance with the school's child protection and safeguarding policy and the relevant Kent Safeguarding Child Multiagency Partnership's procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF) or Kent Police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- Ensure that the Designated Safeguard Lead (or Deputy) 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 children have been found on the school devices, the school will:

- Ensure that the Designated Safeguard Lead (or Deputy) 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 Children's Social Services (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 children on school devices, the school will:

- Ensure that the Headteacher is informed in line with our Managing Allegations Against Staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
- Quarantine any devices until police advice has been sought.

8.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Borden Grammar School.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.

8.4 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Borden Grammar School and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead (or Deputy) will obtain advice through the Education Safeguarding Service and/or Kent Police.

8.5 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead (or Deputy) will be informed immediately and action will be taken in line with the Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.

9.0 Useful Links for Educational Settings

- Rebecca Avery, Education Safeguarding Advisor (Online Protection)
- Online Protection /E-Safety Development Officer
  Tel: 03000 415797/ 07789 968705
- LADO Team: 03000 41 08 88
- Guidance for Educational Settings:
  - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials

- www.theeducationpeople.org/blog/covid-19-online-safeguarding-resources-for-educational-settings-and-parents

KSCB:

- 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 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

National Links and Resources for 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