BORDEN GRAMMAR SCHOOL

Online Safety Policy

Date Drawn up	**October 2010**
Drawn up by	**Michelle Brooker based on The Education People Child Protection policy template September 2021**
Revised by	**Michelle Brooker**
Date Revised	**December 2021**
Date Ratified by Trustees (C&L committee)	**June 2023**
School Online Safety Co-Ordinator (and DSL)	**Michelle Brooker**
School Online Safety Link Trustee	**Mark Bailey**
Frequency of Review	**Annually**
Review Date	**June 2024**

Online Safety Policy

Contents Page

1 Policy Aims and Scope

1.1.1. This online safety policy has been written by Borden Grammar School, involving staff, pupils and parents/carers, building on 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', 'Working Together to Safeguard Children' and the Kent Safeguarding Children Multi-Agency Partnership (KSCMP) procedures.

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 online safety is an essential part of safeguarding and acknowledges our duty to ensure that all learners and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate our learners and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

- Borden Grammar School understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
    - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
    -

1.1.5 Borden recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online

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 technology including computers, tablets, mobile phones, games consoles, smart watches and social media are part of everyday life for all students and staff. This presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

1.1.7 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)

- Anti-bullying policy
- Acceptable Use Policy (AUP)
- Staff Behaviour policy – Code of Conduct
- Safeguarding and Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Personal Social and Health Education (PSHE) and Relationships and Sex Education (RSE)
- Data protection policy
- School image use policy
- Mobile and Social Media Policy

2. Responding to Emerging 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:
    - carry out an annual review of our online safety approaches which will be supported by an annual audit which considers and reflects the specific risks our learners face,
    - 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 is permitted,
    - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet 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, and as such identify clear procedures to follow if breaches or concerns arise.

3. Monitoring and Review

3.1 The policy will be monitored in the following manner:

The E-Safety policy was approved by the Board of Trustees' Pastoral and Wellbeing Sub-Committee:	June 2023
The implementation of the E-Safety policy will be monitored by an E-Safety Group:	Michelle Brooker (AHT & DSL) Rebecca Powell (AHT & deputy DSL) Chris Brinn (AHT & deputy DSL) Natalie Zarzycki (SENCO and deputy DSL) Angela Bryant (HoD ICT) Julian Pilford-Bagwell (Network Manager) Mark Bailey (School Online 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 P&W Sub- Committee.
Monitoring of filtering and control logs	Network Manager (termly)
Logs of Reported Incidents monitored by Designated Safeguarding Lead and Deputy DSLs	Michelle Brooker (termly) Rebecca Powell (AHT & deputy DSL) Chris Brinn (AHT & deputy DSL)
Online Staff Training Updates	Michelle Brooker (annually)

.2 Reviewing the Online Safety Policy

- will review this policy at least annually. The policy will also be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Trustee for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider Trustee body..
- ny issues identified will be incorporated into our action planning.

4. Roles and Responsibilities

4.1 Key Responsibilities of the School Community

- The Designated Safeguarding Lead (DSL) Michelle Brooker is recognised as holding overall lead responsibility for online safety, however 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.

4.1 Key responsibilities of the senior leadership team are to:

- Create a whole school culture that incorporates online safety throughout.
- 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 which address the acceptable use of technology, child-on-child abuse, use of social media and mobile 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.
- 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.
- 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 school curriculum which enables all learners to develop an appropriate understanding of online safety.

4.2 Key responsibilities of The Designated Safeguarding Lead (DSL):

- To act as a named point of contact on all online safety issues.
- Liaise with other members of staff such as pastoral support, IT technicians, network manager and the SENCo on matters of online safety as appropriate.
- Ensure referrals are made to relevant external partner agencies, as

appropriate.
- To work alongside deputy DSLs to ensure online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated whole school approach is implemented.
- To 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, including the additional risks that learners with SEN and disabilities (SEND) face online.
- To 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, e.g. Prevent Online Training.
- To keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- To work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- To ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- To maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- To monitor online safety incidents to identify gaps and trends, and use this data to update the education response, and school policies and procedures.
- To report online safety concerns, as appropriate, to the senior leadership team and Board of Trustees.
- To work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- To meet three times a year with the trustee with a lead responsibility for safeguarding and/or online safety.

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

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs.
- 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 school's 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.

4.4 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 as directed by the leadership team to ensure that the school's IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the school's 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 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.

4.5 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 opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school's acceptable use of technology and behaviour policies.
- Respect the feelings and rights of others, both 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.

4.6 It is the responsibility of parents and carers to:
- Read our 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 reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media, and abide by the school's home-school agreement and acceptable use of technology 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 online issues.
- Contribute to the development of the school's online safety policies.
- 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 that their children access and use at home.

5.Education and Engagement Approaches

5.1 Education and engagement with learners

Borden will establish and embed a whole school culture and will empower our learners to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. We 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 PSHE, RSE and ICT programmes of study.
- Reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
- implementing appropriate peer education approaches, e.g. through use of Online Safety ambassadors in Sixth Form.

- 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 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. Using External Visitors to Support Online Safety Education: Guidance for Educational Schools
- Providing online safety education and training as part of the transition programme across the key stages.

The school will support learners to read and understand and follow our Acceptable Use policies in a way which suits their age and ability by:

- sharing our acceptable use policies with them in accessible and appropriate ways.
- 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.

Borden 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.
- enabling them to understand what acceptable and unacceptable online behaviour looks like.
- 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.
- 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.

5.2 Vulnerable Learners

- Borden Grammar School recognises that any learner can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some learners, for example, looked after children, child who are care leavers, children who are adopted, children who are, or who are perceived to be, lesbian, gay, bi, or trans (LGBT), and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.
- Borden Grammar School will ensure that differentiated and appropriate online safety education, access and support is provided to all learners who require additional or targeted education and/or support.
- Staff at Borden will seek input from specialist staff as appropriate, including the DSL, SENCo, Head of IT, Head of PSHE to ensure that the policy and curriculum is appropriate to our community's needs.

5.3 Training and engagement with staff

The school will:

- Provide and discuss the online safety policy and procedures, including our Acceptable Use policy with all members of staff including Trustees as part of induction.
- Provide up-to-date and appropriate online safety training for all staff including Trustees which is integrated, aligned and considered as part of our overarching safeguarding approach. This is as part of the school's annual safeguarding training, delivered at the start of term 1, and available to all new staff throughout the academic year.
- ensure our training for Trustees equips them with the knowledge to provide strategic challenge to test and assure themselves that our online safety policies and procedures in place in are effective and support the delivery of a robust whole school approach.
- Ensure our training covers the potential risks posed to learners (content, contact and conduct) as well as our professional practice expectations.
- build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
- ensure staff are aware that school IT systems are monitored and that 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.
- ensure staff are 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 school community.

5.4 Awareness and engagement with parents and carers

Borden Grammar School recognises that parents and carers have an essential role to play in enabling our learners to become safe and responsible users of the internet and associated technologies. providing information and guidance on online safety in a variety of formats,

We will ensure parents and carers understand and are aware of:

- the systems used at school to filter and monitor their child's online use by parentmail information, the safeguarding sections of the school website, and through parental events.
- what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online by providing information in our AUP.

We will build a partnership approach and reinforce the important of online safety through regular contact and communication with parents and carers by:

- providing information and guidance on online safety in a variety of formats
- drawing their attention to the school's online safety policy and expectations in our newsletters and other external communication, as well as in our prospectus and on our website.
- requesting parents and carers read online safety information as part of joining our community, i.e. within our home school agreement.
- requiring them to read the school's acceptable use policies and discuss the implications with their children.

6.0 Safer Use of Technology

6.1 Classroom Use

Borden Grammar 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
- School learning platform (Moodle) /intranet, Google Suite
- Email
- Games-based technologies
- Digital cameras, webcams 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. The school uses Google which filters inappropriate content through 'Google Safe Search'.
- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place. This includes YouTube and Vimeo which are filtered by Google Education and our own school filtering system.
- The school 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. This means that learners will use age-appropriate search engines and online tools. Learners will also be appropriately supervised when using technology, according to their ability and understanding.

6.2 Managing Internet Access

- All users will read, agree and acknowledge and sign our Acceptable Use Policy appropriate to their age, understanding and role, before being given access to the school computer system, IT resources or internet.
- The school will maintain a written record of users who are granted access to the school's devices and systems.

6.3 Filtering and Monitoring

6.3.1 Decision Making

- Borden Grammar School will do all we reasonably can to limit children's exposure to online risks through school provided IT systems/devices and will ensure that appropriate filtering and monitoring systems are in place.
- Borden Grammar School Trustees and leaders have ensured that the 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.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- 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 and other relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- Trustees 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.

6.3.2 Appropriate Filtering

- Borden's educational broadband connectivity is provided through BT Internet.
- The school uses Diladele Web Safety filtering system which 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 contact, pornography content and violent material.
- The Diladele Web Safety filtering system is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
- Diladele Web Safety integrates the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

We will work with BT Internet and Diladele Web Safety filtering system 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:

- turn off monitor/screen and report the concern immediately to a member of staff who will pass this to the DSL or deputies.
- The member of staff will report the concern
- Report the URL of the site (if possible) to technical staff to remove it.
- Filtering breaches will be recorded and escalated as appropriate in line with existing policies, including Child Protection, Acceptable Use and behaviour..
- Parents/carers will be informed of filtering breaches involving their child.
- Any access to material that the school believes to be illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police and/or NCA-Child Exploitation and Online Protection Command (CEOP)..

6.3.3 Appropriate 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 logfile 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.
- If a concern is identified via our monitoring approaches:
    - Where the concern relates to learners, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour.

- Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behaviour and allegations policy.

6.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with UK General Data Protection Regulation (GDPR UK) and the Data Protection Act 2018**.** Full information can be found in our GDPR policy which can be accessed on the Policies page of the school website.

6.5 Information Security and Access Management

The school takes appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and learners. Further information about technical environment safety and security can be given by contacting the IT team, but include the following.

- 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.
- Regularly checking files held on the school's network, as required and when deemed necessary by leadership staff.
- The appropriate use of user logins and passwords to access the school network, and 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.
- Reviewing the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies.
- Further information about technical environment safety and security can be found in the Acceptable Use Policy

6.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access the school systems; members of staff are responsible for keeping their password private.
- From Year 7 all learners are provided with their own unique username and private passwords to access the school's systems; learners are responsible for keeping their passwords private
- We require all users to:
    - Use strong passwords for access into our system
    - Not share passwords or login information with other, 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.

6.6 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 learner's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.7 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 School Image Use policy, AUPs, codes of conduct,/ behaviour, social media and use of mobile phones and devices policies.

6.8 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/ 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.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the school community will immediately report offensive communication to the DSL.
- 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.
- We will have a dedicated email for reporting wellbeing and pastoral issues (wellbeing@bordengrammar.kent.sch.uk) . This inbox will be managed by designated and trained staff.

6.8.1 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 school business is not permitted.
- are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and learners and parents.

6.8.2 Learner email

Learners will:

- use a school provided email account for educational purposes.
- agree an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.9 Educational use of Videoconferencing and/ or webcams

- Borden Grammar School recognises that videoconferencing and use of webcams can be a challenging activity, but brings a wide range of learning benefits, e.g. Google Meet, MS Teams, Zoom.
- 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.
- School videoconferencing equipment will not be taken off the school premises without prior permission from the DSL and Headteacher.
- 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.

6.9.1 Users

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

6.9.2 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.

6.10 Management of Learning Platforms

- Borden Grammar School uses Google Suite as its official learning platform and all access and use takes place in accordance with our acceptable use policies.
- 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, learners and parents will have access to the LP. When staff and/or learners' leave the school, their account will be disabled or transferred to their new establishment.

- 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 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 as part of an agreed focus or a limited time slot.

6.11 Management of Applications (apps) used to record progress

- The school uses Edulink to track learner's progress and share appropriate information with parents and carers. It also uses 4Matrix and Alps to track GCSE and A Level pupil progress.
- The Headteacher 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 UK General Data Protection Regulation (GDPR UK) and the Data Protection legislation.

In order to safeguard learner's data:

- Only learner 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.

6.12 Management of Remote Learning

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 provided or approved communication channels; for example, school 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, code of conduct and AUP.
- When delivering remote learning, staff will follow our Remote Learning 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 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.

7.0 Social Media

7.1 Expectations

- Borden Grammar School believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline and all members of our community are expected to engage in social media in a positive and responsible manner.
- The expectations regarding safe and responsible use of social media applies to all members of Borden Grammar School community. The policy applies to all use of social media, the term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger apps or other online communication services.

- All members of our 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 provided devices and systems on site.
- 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 action.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL and/or Headteacher prior to use. Any use will take place in accordance with our Acceptable Use Policy.
- Concerns regarding the online conduct of any member of Borden Grammar School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff (disciplinary policy), behaviour, home-school agreements, staff behaviour code of conduct, AUPs and child protection policies.

7.2 Staff Use of Social Media

- The use of social media during school hours for personal use is not permitted for staff.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our staff behaviour code of conduct policy and acceptable use of technology policy.
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and Staff Behaviour – Code of Conduct.

7.2.1 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 sites. This may 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 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 being linked with the setting and also to safeguard the privacy of staff members.
- All staff are expected 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. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- 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 group immediately if they consider that any content shared on social media sites conflicts with their role in the school.

7.2.2 Communicating with learners and their families

- Staff will not use any personal social media accounts to contact learners or their family members.
- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL (or deputy) and the Headteacher.
- If ongoing contact with learners 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.
- Any communication from learners and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) and the Headteacher.

7.3 Official Use of Social Media

- Borden Grammar School's official social media channels are Facebook, Twitter, Instagram, YouTube.

- The official use of social media sites by Borden Grammar School only takes place with clear educational or community engagement objectives and with specific intended outcomes and the use has been formally risk assessed and approved by the headteacher prior to use.
- Official social media sites are suitably protected and, where possible, run and linked to our website.
    - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media use 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. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- 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.
- Parents and carers will be informed of any official social media use with learners; any official social media activity involving learners will be moderated if possible 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.
- 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 managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read and understand our Acceptable Use Policy.
    - Where they are running official accounts, sign our social media Acceptable Use Policy
    - Be aware they are an ambassador for the school.
    - 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.
    - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
    - 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 or direct messaging with current or past learners or their family members.
    - Inform their line manager, the DSL (or deputy) and/or the headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

7.4 Learners' Use of Social Media

- The use of social media during school hours for personal use is not permitted for learners, with the exception of permission only during lunch/ break times or with specific permission.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a

risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another learner, could have repercussions for the orderly running of the school when the learner is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our Behaviour and Safeguarding & Child Protection and online safety policies.

- Borden Grammar School will empower our learners to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies, e.g. computing.
- 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.
- 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, for example 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.
- Any concerns regarding learners use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to learners as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- 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.

8.0 Mobile and Smart Technology

8.1 Safe Use of mobile and smart technology expectations

- Borden Grammar School recognises that use of mobile and smart technologies is part of everyday life for many learners, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Borden 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.
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices
- Mobile phones and personal devices are not permitted to be used in specific areas such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via personal smart

devices and mobile phones is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.

- All members of the Borden community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene the school's Behaviour or Child Protection policies.

8.2 School Provided mobile phones and devices

- Members of staff will be issued with a work phone number in addition to their work email address, where contact with learners or parents/carers is required. Staff providing formal remote/online learning will do so using school provided equipment in accordance with our AUP**.**
- 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 our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies.
- Where staff and/ or learners are using school provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

8.3 Staff Use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as, relevant school policy and procedures, such as: Confidentiality, Child Protection, data security, staff behaviour code of conduct and AUP.

  Staff will be advised to:

  - Keep mobile phones and personal devices in a safe and secure place during lesson time , switched off or switched to silent mode..
  - 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 permission has been given by the Headteacher, such as in emergency circumstances.
  - Ensure that any content brought onto site via mobile phones and personal devices is compatible with their professional role and the school's behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners 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.
- It is advised that staff should use school owned technology to access Google and Edulink. If staff use a non-school device to access any applications that access confidential information on any non-school devices, they must use due diligence to make certain this information is not accessible by anyone else other than themselves. **At the very minimum, all non-school devices should have two 'levels' of password protection i.e. 2 factor authentication.**
- Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this will be discussed with the DSL and Headteacher.
- Staff will only use school provided equipment (not personal devices):
  - to take photos or videos of learners in line with our image use policy.

- to work directly with learners during lessons/educational activities.
- to communicate with parents/carers.

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and Remote Learning policy.
- If a member of staff breaches the school policy, action will be taken in line with the staff behaviour 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 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.

8.4 Learners use of mobile and smart technology

- Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies, e.g. computing.
- Mobile phones and/or personal devices will not be used on site by learners, e.g.:
    - 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.
    - Staff will only allow learners to use their mobile phones or personal devices as part of an educational activity, following a risk assessment, with approval from the Leadership team.
    - Mobile phones or personal devices can be used by learners during break or free time, but any use must be in accordance with our anti-bullying and behaviour policy. If learners breach our policies, this may be revoked.
- Borden Grammar School expects learners' personal devices and mobile phones to be kept safe and secure when on site. This means:
    - Switched off, have certain functions disabled whilst on site, kept out of sight during lessons and while moving between lessons.
- If a learner needs to contact their parents or carers whilst on site, they will be allowed to use a school phone at main reception.
        - Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher
- If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the Headteacher prior to use being permitted.
    - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.
    - Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents/ carers before use is permitted.

- Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with the AUP and the remote learning policy.

- Mobile phones and devices including but not limited to smartwatches and Fitbits, must not be taken into examinations, and will be handed to the invigilators. Learners found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the learner's withdrawal from either that examination or all examinations.

8.5 Screening, searching and confiscation of electronic devices

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

- Where there are concerns regarding learner's use of mobile technology or policy breaches they will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.
    - staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene the school's child protection, behaviour or anti-bullying policy
    - Mobile phones and devices that have been confiscated will be held in a secure place, e.g. the school office, and released to parents or carers at the end of the school day.
    - Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.
    - If there is suspicion that data or files 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.
    - if deemed to be necessary and appropriate, searches of mobile phones or personal devices will be carried out in accordance with our Searching, Screening and Confiscation policy and in line with the DfE **Searching, Screening and Confiscation'** guidance.
- **Leadership Group** will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a Learner's electronic device that they reasonably suspect are likely to put a person at risk.
- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a pupil/student was in possession of prohibited items, as identified in our behaviour policy (link).
- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupils/student's device has revealed a safeguarding risk.
- In exceptional circumstances and in accordance with our behaviour policy (link) and the DfE 'Searching, Screening and Confiscation' guidance, the headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so. **'Searching, Screening and Confiscation'** pages (77 – 79).

- If the headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

8.4 Visitors' use of mobile and smart technology

- Parents, carers and visitors (including volunteers and contractors) are expected to ensure that their mobile phones and personal devices are only permitted for specific purposes, e.g. as part of multi-agency working arrangements.
- Visitors (including volunteers and contractors) who are on site for a regular or extended period of time are expected to use mobile and smart technology in accordance with our Acceptable Use Policy and other associated policies, such as child protection.
- If visitors require access to mobile and smart technology, for example when working with learners as part of multi-agency activity, this will be discussed with the headteacher prior to use being permitted.
- Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school. This may include undertaking appropriate risk assessments if necessary.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or Headteacher of any breaches of school policy.

9.0 Responding to Online Risks and/or Policy Breaches

- 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 any content, comments, images or videos which could cause harm, distress or offence.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
    - will respect confidentiality and the need to follow the official school procedures for reporting concerns.
    - will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
    - will be made aware of how the school will monitor policy compliance by: AUPs, staff training, filtering system reports.
    - are expected to adopt a partnership with the school to resolve issues.
- If appropriate, after any investigations are completed, the DSL and leadership staff 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 Headteacher will seek advice from the local authority or the Education Safeguarding Service.

9.1 Concerns about learner online behaviour and/ or welfare

- Borden recognises that an initial disclosure to a trusted adult may only be the first incident reported, rather than representative of a singular incident and that trauma can impact memory, so children may not be able to recall all details or timeline of abuse. All staff will be aware certain children may face additional barriers to telling someone, for example because of their vulnerability, disability, sex, ethnicity, and/or

sexual orientation.

- All concerns about learners will be responded to and recorded in line with our child protection policy:
    - The DSL will be informed of any online safety incidents involving safeguarding or child protection risks in line with our child protection policy.
    - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with the Kent Safeguarding Children Multiagency Partnership (KCSMP) thresholds and procedures
- Abuse that occurs online and/or offsite will not be dismissed or downplayed; concerns will be treated equally seriously and in line with relevant policies/procedures, for example Anti-Bullying, Behaviour, Safeguarding& child protection, online safety.
- Borden recognises that the law is in place to protect children and young people rather than criminalise them, and this will be explained in such a way to learners that avoids alarming or distressing them.
- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to learners as appropriate. Civil or legal action will be taken if necessary.
- The school will inform parents/ carers of any incidents or concerns involving their child, as and when required.

9.2 Concerns about staff online behaviour and/ or welfare

- Any complaint about staff misuse will be managed in accordance with our Staff Behaviour - Code of Conduct policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with the staff behaviour code of conduct policy.

9.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

10.0 Procedures for responding to specific online incidents or concerns

10.1. Online child-on-child abuse

- Borden Grammar School recognises that whilst risks can be posed by unknown individuals or adults online, learners can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our child protection and behaviour policies.
- We recognise that online child-on-child abuse can take many forms, including but not limited to:
    - bullying, including cyberbullying, prejudice-based and discriminatory bullying
    - abuse in intimate personal relationships between peers

    - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
    - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
    - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
    - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
    - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
    - initiation/hazing type violence and rituals.
- Borden Grammar School adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse, including when it takes place online and it will never be tolerated or dismissed as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children and a culture that normalises abuse, which can prevent children from coming forward to report it.
    - Borden believes that all staff have a role to play in challenging inappropriate online behaviours between children.
- Borden recognises that, even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.
    - Concerns about learner's behaviour, including child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with learners and parents/carers and in line with existing policies, for example anti-bullying, acceptable use, behaviour and child protection policies. Section 89(5) of the Education and Inspections Act 2006 gives headteachers a statutory power to discipline pupils for poor behaviour outside of the school premises e.g. when children are not under the lawful control or charge of a member of school staff, to such extent as is reasonable. This legislation is not applicable to independent schools.
    - Borden wants children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child-on-child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-bullying and behaviour. Learners who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

10.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Borden will follow the guidance outlined in Part Five of KCSIE and the DfE **www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals**
- guidance.
- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed
- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.

- Borden recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - 'upskirting' (which is a criminal offence and typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.
- Borden recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services, and for things to move from platform to platform online.
- Borden 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.
- Borden 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.
- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.
    - Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the Police and the Education Safeguarding Service.
    - The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
- If content is contained on learners' personal devices, they will be managed in accordance with the DfE '[searching screening and confiscation']' advice.

Following an immediate risk assessment the school will:

- provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- review the handling of any incidents to ensure that best practice was implemented, and policies/ procedures are appropriate.
- inform parents /carers for all children involved about the incident and how it is being managed, and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm,
- 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 will discuss this with the police first to ensure that investigations are not compromised.

- Borden recognises that the internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Borden also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

10.1.2 Nude or semi-nude image sharing

- The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18. Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing, and should be read and understood by DSLs working will all age groups, not just older learners.
- Borden Grammar School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
  - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
  - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
  - possesses nude and/or semi-nude imagery created by another person under the age of 18.
- When made aware of concerns regarding nude and semi-nude imagery, Borden will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- Borden Grammar School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.
- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
  - Report any concerns to the DSL immediately.
  - Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery, this will be immediately reported to the DSL.
  - Not delete the imagery or ask the child to delete it.
  - Not say or do anything to blame or shame any children involved.
  - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.

- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
  - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
  - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of learners involved, including the possibility of carrying out relevant checks with other agencies.
  - a referral will be made to Children's Social Care and/or the police immediately if:
    - the incident involves an adult (over 18) **to discuss with Trustees whether parents should be notified as well, e.g. for Year 13 students**
    - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
    - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
    - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
  - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
  - If DSLs are unsure how to proceed, advice will be sought from the local authority. e.g. the Education Safeguarding Service.
  - Store any devices 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.
  - inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm. **To discuss with trustees whether Sixth form parents are informed if student is over 18**
  - provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
  - implement sanctions where necessary and appropriate 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.
    - Learners will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
  - 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.

We will not:

- view any imagery, unless there is no other option or there is a clear safeguarding need or reason to do so. DSLs should follow 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, 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 and will not allow or request learners to do so.

10.1.3 Cyberbullying

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

10.2 Online child abuse and exploitation

- Borden 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, in line with our child protection policy.
- Borden 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.
- 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.

If made aware of an incident involving online child abuse and / or exploitation, we will:

- act in accordance with child protection policies and the relevant local Kent Safeguarding Child Multiagency Partnership's procedures.
- store any devices containing evidences 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 school 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 the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police. e.g. the Education Safeguarding Service.
- We will ensure that the NCA-CEOP reporting tools are visible and available to learners and other members of our community, e.g. on the school website.
- 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.

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

10.3 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) as appropriate.
- We will respond to concerns regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school 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 the school is unclear if a criminal offence has been committed, the DSL 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 safeguarding and child protection policy and the Kent Safeguarding Child Multiagency Partnership's procedures.
- store any devices involved securely until advice has been sought. If content is contained on learners' personal devices, they will be managed in accordance with the DfE **'searching screening and confiscation'** advice.
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent Police or the LADO.

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

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the IWF via www.iwf.org.uk and/or police.
- inform the police as appropriate, for example if images have been deliberately sent to or shared by learners.
- report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the school provided devices, the school will:

- ensure that the DSL 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 (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) following a written request from the police
- 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 Staff behaviour- Code of Conduct policy
- Inform the LADO and other relevant organisations, such as the police, in accordance

with the school's Staff behaviour- Code of Conduct policy
- quarantine any involved school provided devices until police advice has been sought.

10.4 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 child protection, 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 DSL will seek advice through the Education Safeguarding Service and/or Kent Police.

10.5 Online radicalisation and extremism

- The school 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 the school is concerned that a learner or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with the school's child protection policy.

10.6 Cybercrime

- Borden Grammar School recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

11.0 Useful Links for Educational Settings

- LADO Team: 03000 41 08 88
- UK Council for Internet Safety (UKCIS): www.gov.uk/government/organisations/uk-council-for-internet-safety
- UK Safer Internet Centre: www.saferinternet.org.uk
- SWGfL: 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
- PSHE Association: www.pshe-association.org.uk
- National Education Network (NEN): www.nen.gov.uk
- National Cyber Security Centre (NCSC): www.ncsc.gov.uk
- Educate against hate: https://educateagainsthate.com
- NCA-CEOP Education Resources: www.thinkuknow.co.uk
- Safer Recruitment Consortium: www.saferrecruitmentconsortium.org/

Reporting Helplines

- NCA-CEOP Safety Centre: www.ceop.police.uk/Safety-Centre
- Internet Watch Foundation (IWF): www.iwf.org.uk
- ChildLine: www.childline.org.uk
  - Report Remove Tool for nude images: www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online
- Stop it now! www.stopitnow.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- Action Fraud: www.actionfraud.police.uk
- Report Harmful Content: https://reportharmfulcontent.com
- Revenge Porn Helpline: https://revengepornhelpline.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Support for children and parents/carers

- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Parent Zone: https://parentzone.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
  - Net Aware: www.net-aware.org.uk
- Parents Protect: www.parentsprotect.co.uk
- Get Safe Online: www.getsafeonline.org
- NCA-CEOP Child and Parent Resources: www.thinkuknow.co.uk