BORDEN GRAMMAR SCHOOL

NITERE PORRO

Acceptable Use Policy

Review Responsibility:	Assistant Headteacher - Safeguarding & Inclusion
Frequency of Review:	3 years
Date Approved:	June 2024
Approved By:	Board of Trustees
Next Review Due By:	June 2027

Key Stage 3/4/5 (11-18)

Learning

- I know that school computers, devices and internet access has been provided to help me with my learning and that other use of technology may not be allowed. If I am not sure if something is allowed, I will ask a member of staff.
- If I need to learn online at home, I will follow the school remote learning Acceptable Use Policy (AUP).
- I will only use my personal device/mobile phone in school if I have permission from a teacher.

Safe

- I will make sure that my internet use is safe and legal and I am aware that online actions have offline consequences
- I know that my use of school computers, devices and internet access will be monitored at school, to protect me and ensure I comply with the school's AUP
- I know that people online aren't always who they say they are and that I must always talk to an adult before meeting any online contacts

Private

- I will keep my passwords private
- I know I must always check my privacy settings are safe and private
- I will think before I share personal information and/or seek advice from an adult
- I will keep my password safe and private as my privacy, school work and safety must be protected. I understand that when I am away from a computer, logged into my user account, I should lock the screen.

Responsible

- I will not access or change other people's files, accounts or information
- I will only upload appropriate pictures or videos of others online when I have permission
- I will only use my personal device/mobile phone in lessons if I have permission from a teacher
- I know I must respect the school's systems and equipment and if I cannot be responsible then I will lose the right to use them
- I know that school computers and internet access has been provided to help me with my learning and that other use of technology may not be allowed e.g the playing of games. If I'm not sure if something is allowed then I will ask a member of staff
- I will write emails and online messages carefully and politely; as I know they could be forwarded or seen by someone I did not intend
- I will only change the settings on the computer if a teacher/technician has allowed me to
- I know that use of the schools ICT system for personal financial gain, gambling, political purposes or advertising is not allowed
- I understand that the school's internet filter is there to protect me, and I will not try to bypass it.

- I know that if the school suspects that I am behaving inappropriately with technology, then enhanced monitoring and procedures may be used, such as checking and/or confiscating personal technologies such as mobile phones.
- I know that if I do not follow the AUP then I will be banned from the school's ICT network for a set period of time or be sanctioned according to the school's behaviour policy.
- I understand that I may not set up any social media site that may purport or seem to be part of an official Borden Grammar School account.

Kind

- I know that bullying in any form (online and offline) is not tolerated and I know that technology should not be used for harassment of any type.
- I will not upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community. I understand that it may be a criminal offence or a breach of the school policy to download or share inappropriate pictures, videos, or other material online. I understand that it is against the law to take, save or send nude or semi-nude images or videos of anyone under the age of 18.
- I will always think before I post as once, I upload text, photos or videos they can become public and impossible to delete.
- I will not use technology to be unkind to people

Legal

- I know cybercrime can be a criminal offence, for example gaining unauthorised access to systems ('hacking') and making, supplying or obtaining malware.
- I know it can be a criminal offence to send threatening and offensive messages.
- I know it can be a criminal offence to hack accounts or systems or send threatening and offensive messages
- I will respect other people's information and copyright by giving a reference and asking permission before using images or text from online sources
- I understand that it may be a criminal offence or breach of the school policy to download or share inappropriate pictures, videos or other material online.
- I understand that the school has the duty to pass on information to the relevant authorities should criminal activity be discovered.

Reliable

- I will always check that any information I use online is reliable and accurate
- I know that people I meet online may not be who they say they are. If someone online suggests meeting up then I will immediately talk to an adult and will always arrange to meet in a public place, with a trusted adult present

Report

- If I am aware of anyone trying to misuse technology then I will report it to a member of staff
- I will speak to an adult I trust if something happens to either myself or another student which makes me feel worried, scared, uncomfortable or is illegal
- I will visit www.thinkuknow.co.uk www.childnet.com and www.childline.org.uk to find out

more about keeping safe online

- I understand it is my responsibility to report any damage, e.g keys missing from keyboards, cracks in screens, to my teacher or directly to the ICT department straight away. If I do not report damage it may lead to me being wrongly accused of causing said damage.
- I understand that deliberate damage to equipment will be treated as a serious breach of regulations and will be charged for.
- I have read and talked about these rules with my parents/carers

Student Acceptable Use Policy Agreement Form The Policy is available on the school's website Policies page

Borden Grammar School Acceptable Use of Technology Policy – Learner Agreement

I, with my parents/carers, have read and understood the school's Acceptable Use of Technology Policy (AUP) and remote learning AUP

I agree to follow the AUP when:

- I use school devices and systems, both on site and at home.
- I use my own devices in school when allowed, including mobile phones, gaming devices, and cameras.
- I use my own equipment out of the school in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school emails, Google suite or other educational platforms the school provides.

Name……………………………………………….
Signed………………………. Class…………………………
Date…………………….
Parent/Carers Name…………………………………………........
Parent/Carers Signature…………………………

Letter for Parents and Carers

Dear Parent/Carer,

All students at Borden Grammar School use computer facilities and internet access, as an essential part of learning as required by our curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes, but is not limited to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Email
- Digital cameras, webcams and video cameras
- Mobile Phones
- Google Suite

Borden Grammar School recognises the essential and important contribution that technology plays in promoting children's learning and development; we believe it offers a fantastic range of positive activities and experiences as well as enabling continued learning during exceptional periods. We do recognise however that this can bring risks. We take your child's online safety seriously and, as such, will take all reasonable precautions, including monitoring and filtering systems, to ensure that students are safe when they use our internet and systems.

We recognise however that no technical system can replace online safety education and believe that children themselves have an important role to play in developing responsible behaviour. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the Acceptable Use Policy which is available on the school's home page with your child, discuss the content with them and return the attached slip.

Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

We request that all parents support our approach to online safety by role modelling safe and positive online behaviour and by discussing online safety whenever children access technology at home. Parents/carers may also like to visit the following links for more information about keeping children safe online:

- www.thinkuknow.co.uk
- www.childnet.com
- www.nspcc.org.uk/onlinesafety
- www.saferinternet.org.uk
- www.internetmatters.org

Should you wish to discuss the matter further, please do not hesitate to contact the school Designated Safeguarding Lead, Mrs Brooker, or Head of Year.

Yours faithfully,

Ashley Tomlin
Headteacher

Parents/Carers Acceptable Use Policy Acknowledgment

Learner Acceptable Use of Technology Policy Acknowledgment.

1. I have read and discussed Borden Grammar School's acceptable use of technology policy (AUP) with my child and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child's use of school devices and systems on site and at home including school emails, Google Suite or other educational platforms the school provides, and personal use where there are safeguarding and/or behaviour concerns. This may include if online behaviour poses a threat or causes harm to another student, could have repercussions for the orderly running of the school, if a student is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school.

3. I understand that any use of school devices and systems are appropriately filtered; this means/includes-
   - Borden's educational broadband connectivity is provided through BT Internet.
   - The school uses Impero Software 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 Impero Software filtering system is a member of Internet Watch Foundation (IWF) and blocks access to illegal Child Abuse Images and Content (CAIC).
   - Impero Software integrates 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.
   - Borden Grammar School will work with BT Internet and Impero Software filtering system to ensure that the filtering policy is continually reviewed to reflect the schools needs and requirements.If learners, or parents 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.
   - 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).
4. I am aware that my child's use of school provided devices and systems will be monitored for safety and security reasons, when used on and offsite. 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.

5. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems as above, to ensure my child is safe when they use school devices and systems, on and offsite. I however understand that the school cannot ultimately be held responsible for filtering breaches that occur due to the dynamic nature of materials accessed online, or if my child is using a personal device, including mobile or smart technologies.

6. I am aware that the school mobile and smart technology policy states that my child cannot use personal devices, including mobile and smart technology on site unless given specific permission from a member of staff.

7. I understand that my child needs a safe and appropriate place to access remote/online learning, for example, if the school is closed. I will ensure my child's access to remote/online learning is appropriately supervised and any use is in accordance with the school remote learning AUP. When accessing video learning, I will ensure they are in an appropriate location (e.g., not in bed) and that they are suitably dressed.

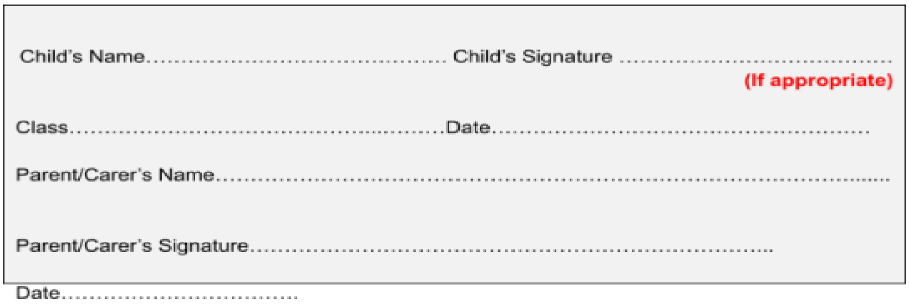
8. I and my child are aware of the importance of safe online behaviour and will not deliberately upload or share any content that could upset, threaten the safety of or offend any member of the school community, or content that could adversely affect the reputation of the school.

9. I understand that the school will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety online.

10. I will inform the school (for example speaking to a member of staff and/or the Designated Safeguarding Lead) or other relevant organisations if I have concerns over my child's or other members of the school community's safety online. I know that I can contact the Designated Safeguarding Lead (Michelle Brooker), my child's form tutor, Head of Year or Headteacher if I have any concerns about online safety.

11. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.

12. I understand my role and responsibility in supporting the school online safety approaches and safeguarding my child online. I will use parental controls, supervise access and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding



Child's Name.. Child's Signature ....

(If appropriate)

Class...Date..

Parent/Carer's Name..

Parent/Carer's Signature..

Date.................................

Staff, Trustee, Visitor and Volunteer Acceptable Use Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Borden Grammar School's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for learners, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Borden Grammar School's expectations regarding safe and responsible technology use, and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

1. Policy Scope

- I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within Borden Grammar School both professionally and personally both on and offsite. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

- I understand that Borden Grammar School's Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school's staff behaviour policy/code of conduct and remote learning policy.

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

2. Use of School Devices and Systems

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

- I understand that any equipment and internet services provided by my workplace is intended for educational use and should only be accessed by members of staff in line with the Staff IT equipment loan agreement. Where I deliver or support remote learning, I will comply with the school's remote learning AUP.

3. Data and System Security

- To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system.
    - I will protect the devices in my care from unapproved access or theft.
- I will respect school system security and will not disclose my password or security information to others.

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

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

- I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school's GDPR policy.
  - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.
  - Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school.
  - I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

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

- I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

- If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Network Manager as soon as possible.

- If I have lost any school related documents or files, I will report this to the IT Network Manager (Julian Pilfold-Bagwell) and the Data Protection Officer (Kirsty Murphy) as soon as possible.

- Any images or videos of learners will only be used as stated in the school Image Use policy.

- I understand images of learners must always be appropriate and should only be taken with school provided equipment and taken/published where learners and their parent/carer have given explicit consent.

4. Classroom Practice

- I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by school as detailed in the online safety policy and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

- If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and ICT network manager.
- I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the Child protection, online safety and remote learning acceptable use policy.
- I will promote online safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where students feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Michelle Brooker) or a deputy (Chris Brinn, Rebecca Powell, Natalie Zarzycki) as part of planning online safety lessons or activities to ensure support is in place for any students who may be impacted by the content.
    - Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with students is appropriate.
- I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

5. Use of Social Media and Mobile Technology

- I have read and understood the school mobile and smart technology and social media sections of the Online Safety Policy which addresses use by students and staff.
- I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff section of the Online Safety Policy and the school mobile technology policy and the law.

6. Online communication, including use of social media

- I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policy, staff behaviour policy/code of conduct, social media policy and the law.

- As outlined in the staff behaviour policy/code of conduct and school social media policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to students, staff, school business or parents/carers on social media.

- My electronic communications with current and past students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via

school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.

  - I will not share any personal contact information or details with students, such as my personal email address or phone number.
  - I will not add or accept friend requests or communications on personal social media with current or past students and/or their parents/carers.
  - If I am approached online by a current or past students or parents/carers, I will not respond and will report the communication to my line manager and (Michelle Brooker) Designated Safeguarding Lead (DSL).
  - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

7. Policy concerns

● I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act. ● I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

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

● I will report and record any concerns about the welfare, safety or behaviour of students or parents/carers online to the DSL in line with the school child protection policy. ● I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school child protection policy and the allegations against staff policy.

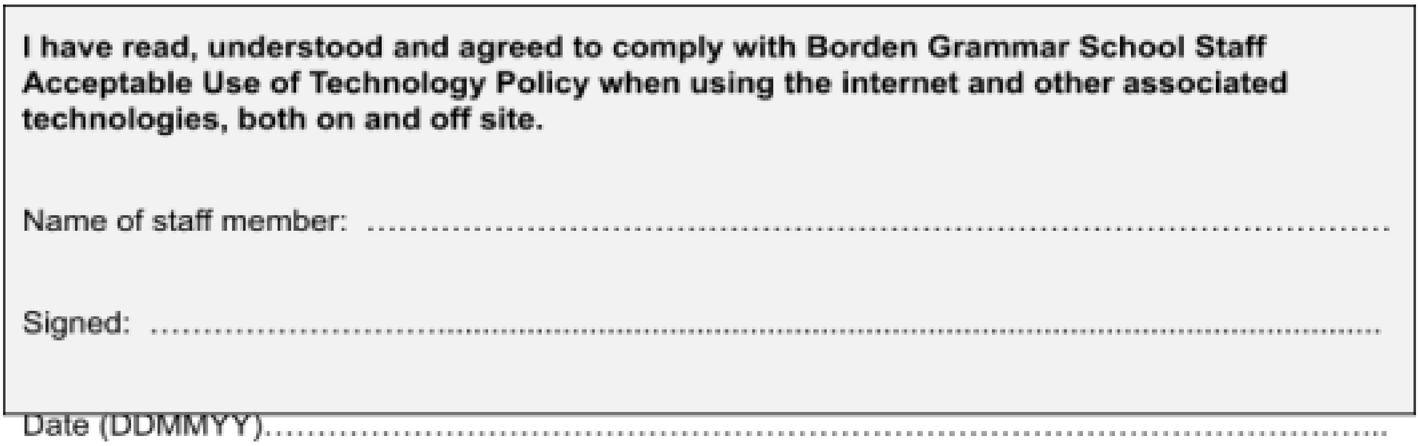
8. Policy Compliance and Breaches

- If I have any queries or questions regarding safe and professional practice online, either in school or off site, I will raise them with the DSL or the headteacher.

- I understand that the school may exercise its right to monitor the use of its devices' information systems to monitor policy compliance and to ensure the safety of students and staff. This includes monitoring all school provided devices and school systems and networks including school provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via school provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

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

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


I have read, understood and agreed to comply with Borden Grammar School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

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

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

Date (DDMMYY)……………………………………………………………………………………

Wi-Fi Acceptable Use Policy

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

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

1. The school provides Wi-Fi for the school community and allows access for **education use only).**

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

3. The use of technology falls under Borden Grammar School Acceptable Use of Technology Policy (AUP), online safety policy and behaviour policy (**any other relevant policies such as data security, child protection, online safety**) which all students /staff/visitors and volunteers must agree to and comply with.

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

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

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

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

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

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

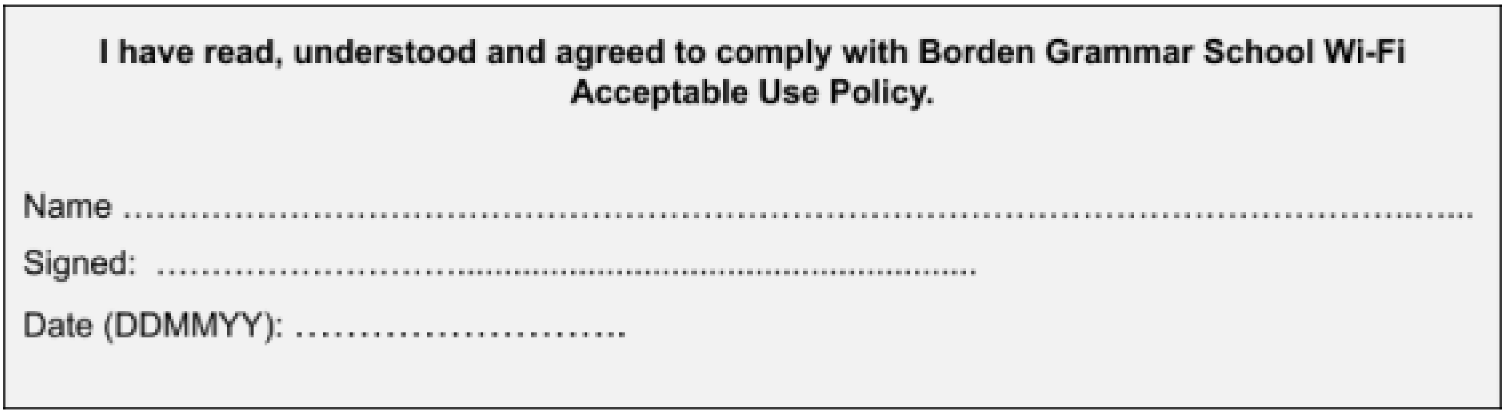
10. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

11. My use of school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

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

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with the Designated Safeguarding Lead (Michelle Brooker) or the headteacher.

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



I have read, understood and agreed to comply with Borden Grammar School Wi-Fi Acceptable Use Policy.

Name ....

Signed: ....

Date (DDMMYY): ....