



Online Safety Policy

Review Responsibility: Assistant Headteacher – Safeguarding & Inclusion

Frequency of Review: 1 year

Date Approved: Sep 26

Approved By: Board of Trustees

Next Review Due By: Sep 27

Contents

1. Aims	4
2. Legislation and Guidance	4
3. Roles and Responsibilities	4
3.1 The Trustees	4
3.2 The Headteacher	5
3.3 The Designated Safeguarding Lead (DSL)	5
3.4 The ICT Manager	6
3.5 All Staff and Volunteers	6
3.6 Parents/Carers	7
3.7 Visitors and Members of the Community	7
4. Educating Pupils	7
4.1 Online Safety	7
4.2 Cyber Security	9
5. Educating Parents/Carers about Online Safety	9
6. Cyberbullying	9
6.1 Definition	9
6.2 Preventing & Addressing Cyber-Bullying	9
6.3 Examining Electronic Devices	10
6.4 Artificial Intelligence (AI)	11
7. Acceptable Use of the Internet in School	11
8. Pupils Using Mobile Devices in School	11
9. Staff Using Work Devices Outside School	12
10. How the School will Respond to Issues of Misuse	12
11. Training	13
Staff, Trustees & Volunteers	13
12. Monitoring Arrangements	13
13. Links with Other Policies	13
Appendix 1 – Acceptable Use Policy	15
1. Student Acceptable Use Policy Agreement	15
Learning	15
Safe	15
Private	15
Responsible	15
Kind	16
Legal	16
Reliable	16
Report	16
2. Parents/Carers Acceptable Use Policy Agreement	17
1. Access to Technology	17
2. Scope of the Pupil AUP	17

3. Understanding the Pupil AUP	17
4. Supporting Safe & Responsible Technology Use	17
5. Mobile Phones & Smart Technology	17
6. Filtering	17
7. Monitoring	18
8. Limitations of Filtering & Monitoring	18
9. Online Safety Education	18
10. Supporting my Child at Home	18
11. Remote & Online Learning	18
12. Positive & Respectful Online Behaviour	18
13. Raising Concerns & Complaints	18
14. Reporting Online Safety Concerns	19
15. Responding to Online Concerns	19
16. Online Safety Advice & Support	19
17. Agreement	19
3. Letter for Parents/Carers	21
4. Student & Parent/Carer Agreement Slip	22
5. Staff, Trustee, Visitor & Volunteer Acceptable Use Policy Agreement	23
Policy Scope	23
Use of School Devices and Systems	23
Data and System Security	23
Classroom Practice	24
Use of Social Media and Mobile Technology	26
Online Communication (including use of social media)	26
Policy Concerns	27
Policy Compliance and Breaches	27

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as 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, such as 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 including those generated by AI and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Meeting digital and technology standards](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- [Relationships and sex education \(RSE\) and health education](#)
- [Searching, screening and confiscation](#)
- <https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools>

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), the [Children's Wellbeing and Schools Act 2026](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Trustees

The trustees have overall responsibility for monitoring this policy and holding the headteacher to account for

its implementation. The board will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

The trustees will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The trustees will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The trustees will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The trustees will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The trustees will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The board will review the [DfE filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The trustee who oversees online safety is Mrs E Sutehall.

All trustees will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances – for example, a confidential shared mailbox to make sure safeguarding concerns are received, monitored and acted on without delay.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and trustees to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing trustees with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are recorded on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety as part of the annual safeguarding training
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or trustees
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking to the DSL and/or raising an incident on CPOMS
- Following the correct procedures by discussing with the ICT Manager and/or DSL if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Help and advice for parents/carers – [Childnet](#)
- Parents and carers resource sheet – [Childnet](#)

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating Pupils

4.1 Online Safety

Pupils will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#) and from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#)

All schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

Secondary schools:

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and/or may

post things which aren't real/have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online

- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- How information and data is generated, collected, shared and used online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.2 Cyber Security

Pupils will be taught practical cyber security skills.

The following items come from the DfE's non-statutory cyber security standards for schools and colleges.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

5. Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online
- The school's expectations in respect of appropriate use of AI by pupils

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher

6. Cyberbullying

6.1 Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites.

Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing & Addressing Cyber-Bullying

To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors will discuss cyber-bullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyberbullying to parents/carers so they are aware of the signs,

how to report it and how they can support children who may be affected.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

The headteacher authorises who can search and at Borden Grammar School these are members of the Leadership Team and, at times, they may be accompanied by a Head of Year or member of the Behaviour Team who are also safeguarding trained. They can carry out a search and confiscate any electronic device, in line with the school's Searching, Screening & Confiscation policy, that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL, headteacher or other member of the Leadership Team
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to DSL, headteacher or other member of the Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- View, copy, print, share, store, save, forward on, or ask a child to share or download, the image
- Delete the image or ask the pupil to delete the image
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any pupil involved

- The staff member will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our Behaviour Policy and Searching, Screening & Confiscation Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Borden Grammar School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deep fakes', where AI is used to create images, audio or video hoaxes that look real. This includes deep fake pornography: pornographic content created using AI to include someone's likeness.

Borden Grammar School will treat any use of AI to bully pupils in line with our Anti-bullying policy and Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI policy.

7. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, trustees and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 and 2.

Smart devices such as smart glasses that record images are not allowed on site from staff, students, parents, visitors, volunteers, contractors or anyone else who enters the school site. It will be at the discretion of a member of the Leadership team if a device falls under this category.

8. Pupils Using Mobile Devices in School

In line with [DfE statutory guidance](#), our school is a mobile phone-free environment by default. Borden

Grammar School upholds a strict **'On Site, Out of Sight, Off'** policy.

Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes, they must be switched off, in their bags and not on their persons (eg. pockets). Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Social times including before school after entering school site, break, lunch and after school before leaving school site.
- Tutor group time
- Clubs before or after school, or any other activities organised by the school
- Sixth form students may access their mobile phones but only in designated sixth form areas such as the sixth form work room and only at social times (before school, after school, break times and lunch times). Sixth-form pupils remain subject to the school's behaviour policy and misuse of their phone may lead to sanctions pursuant to the school's behaviour policy.

There are exceptions for educational/medical needs that may require additional support via their mobile phone. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

This does not include the use of laptops or tablets for learning. These devices should be used in accordance with our Acceptable Use Policy.

9. Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Acceptable Use Policy (Appendix 1) and Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

Staff, Trustees & Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, including images generated or altered by AI, especially around chat groups
 - Sharing of abusive images and pornography, including images generated or altered by AI, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety on the safeguarding platform. CPOMS and /or the filtering and monitoring log.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the trustees. The review will be supported by an annual checking of provision that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- AI Policy
- Acceptable Use Policy (Appendix 1)
- Anti-Bullying Policy
- Behaviour Policy

- Complaints Procedure
- GDPR UK & Data Protection Policy and Privacy Notices
- Mobile Phone & Devices Policy
- Relationship & Sex Education (RSE) Policy
- Safeguarding & Child Protection Policy
- Searching, Screening & Confiscation Policy
- Staff Disciplinary Policy & Procedure
- Whistleblowing Policy

Appendix 1 – Acceptable Use Policy

1. Student Acceptable Use Policy Agreement

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

Learning

- I know that school computers, devices and internet access have 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 use Artificial Intelligence (AI) tools responsibly and only when allowed by a member of staff. I won't use them to cheat, copy other people's work, or create anything unkind or inappropriate. I understand that AI doesn't always give correct or fair answers, so I will check information and ask for help if I'm unsure.
- I understand that under government guidance, mobile phones should not be used in school and I cannot use my mobile phone, even for educational purposes (with the exception of sixth form and use in designated areas/medical purposes).

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 Borden Grammar School provided devices, accounts, systems and internet access will be monitored to help keep people and systems safe and to check that I am following the 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 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 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.
- If there are concerns about how I have used technology or a personal device, the school may look into

what has happened and respond in line with its policies. This may include taking or checking a device where the school is permitted to do so.

- 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 at Borden Grammar School and I know that technology should not be used for harassment of any type.
- I will not use technology to threaten, bully, harass, humiliate, impersonate or deliberately cause harm to another person, or create or share content that risks someone's safety or wellbeing.
- 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 text, photos or videos 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 for example, by giving a reference/source, ensuring any work submitted is my own, 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 safe 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 a safe adult if something happens to either myself or another student which makes me feel worried, scared, uncomfortable
- I will visit www.ceopeducation.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

2. Parents/Carers Acceptable Use Policy Agreement

1. Access to Technology

I understand that my child will be provided with internet access and may use a range of technology, devices, accounts and online services at school to support their learning, development and preparation for life in a digital world.

2. Scope of the Pupil AUP

I understand that the Pupil AUP applies to my child's use of school-provided devices, accounts, systems and internet access, both on site and when accessed away from the school.

Relevant school expectations may also apply to personal technology use where online behaviour:

- affects the safety or wellbeing of a child, member of staff or another person;
- disrupts the safe or effective operation of the school; or
- raises a safeguarding, behaviour or potentially unlawful concern.

3. Understanding the Pupil AUP

I have received and read the Acceptable Use of Technology Policy and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.

4. Supporting Safe & Responsible Technology Use

I will support my child to understand and follow the school's expectations for safe, kind, lawful and responsible use of technology. This includes expectations relating to online communication, social media, images and recordings and, where relevant, artificial intelligence tools.

I understand that guidance, legislation, technology and online risks may change and that the school may review and update its policies and expectations in response.

5. Mobile Phones & Smart Technology

I am aware that the school has clear expectations concerning children's use of mobile phones and smart technology.

In schools, pupils should not use, access, display or check mobile phones or similar smart technology during the school day, including during lessons, time between lessons, breaktimes and lunchtime, unless a specific exception or reasonable adjustment has been agreed.

Where my child may need access to a mobile phone or smart device because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school. Any exception or reasonable adjustment will be considered individually and, where agreed, the purpose, arrangements and expectations for use will be clearly recorded and communicated to my child and relevant staff.

I will support the school's expectations and any individual arrangements agreed for my child. I will not contact my child directly on their mobile phone or smart device during the school day unless this forms part of an agreed arrangement. If I need to contact my child during the day, I will use the school office or another agreed contact route.

6. Filtering

I understand that access to online content through school-provided devices, systems and internet services is appropriately filtered. Information about the filtering arrangements in place can be made available upon request to the DSL.

7. Monitoring

I am aware that my child's use of school-provided devices, accounts and systems may be monitored, including when those devices, accounts or systems are used away from the school. Information about the monitoring arrangements in place can be made available upon request to the DSL.

Monitoring is used to help keep children safe, protect systems and check compliance with relevant policies. It will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

8. Limitations of Filtering & Monitoring

I understand that the school will take reasonable and proportionate steps, including the use of appropriate filtering and monitoring arrangements, to help keep children safe when using school-provided devices and systems.

I understand that no filtering or monitoring system can remove every online risk, particularly where online content changes rapidly or where children use personal devices, accounts, networks or services outside the school's systems.

9. Online Safety Education

I understand that my child will receive age and ability-appropriate online safety education to help them use technology safely and responsibly, both within and outside the school.

I recognise that education, appropriate supervision, open communication and opportunities to seek help remain important alongside technical measures such as filtering and monitoring.

10. Supporting my Child at Home

I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will:

- consider the use of suitable parental controls and safety settings;
- provide appropriate supervision, support and guidance;
- talk to my child about their online experiences;
- encourage safe, kind, lawful and responsible online behaviour; and
- help my child understand how and where to seek support.

11. Remote & Online Learning

Where my child accesses remote or online learning, I will support them to follow the school's remote/online learning expectations. I will help my child to access learning from an appropriate location and provide supervision and support that reflects their age, understanding and needs.

I understand that the school will provide information about the systems and sites my child is expected to access and who from the school, if anyone, they will interact with online.

12. Positive & Respectful Online Behaviour

I will support the school's approach to online safety and model safe, positive and respectful online behaviour, including when creating or sharing images, text, audio or video.

I will support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school community.

13. Raising Concerns & Complaints

If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that the matter can be properly understood and considered.

14. Reporting Online Safety Concerns

I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff.

This may include:

- Head of Year;
- The Designated Safeguarding Lead; or
- The Headteacher.

Where necessary, I may also report the concern to another relevant organisation or emergency service.

15. Responding to Online Concerns

If the school has concerns about my child's online safety, online behaviour or use of technology, I understand that these will be considered fairly and proportionately under the setting's child protection, behaviour and other relevant policies.

The school may also need to consider an appropriate response where online behaviour involving a parent/carer affects the safety or wellbeing of a child, member of staff or another person; disrupts the safe or effective operation of the school; involves confidential or personal information; or raises a safeguarding or potentially unlawful concern. Any such concern will be considered fairly and proportionately, taking account of the particular circumstances and in line with the school's procedures or other relevant arrangements.

The school will communicate with those involved where it is appropriate and safe to do so. I understand that there may be circumstances in which the setting must first follow its safeguarding procedures or seek advice from another agency. Where behaviour may be unlawful or presents a risk to safety, the school may seek appropriate safeguarding, police or legal advice.

16. Online Safety Advice & Support

I know that I can seek information or support from the school about online safety and helping my child to use technology safely. Information is available through various outlets including termly newsletters, safeguarding information, help guides and contacting the schools pastoral systems.

17. Agreement

- I confirm that I have read and understood the Borden Grammar School Parent/Carer Acceptable Use of Technology Policy and agree to support its expectations and the safe, lawful and responsible use of technology by my child.
- I have received and read the Borden Grammar School Pupil Acceptable Use of Technology Policy (AUP) and have discussed its expectations with my child in a way that is appropriate to their age, understanding and needs.
- I understand that the AUP explains how my child is expected to use technology safely, kindly, lawfully and responsibly, including when using:
 - school-provided devices, accounts, systems and internet access;
 - school-provided technology away from the setting;
 - personal devices or services where their use affects the safety or wellbeing of a child or another person, disrupts the safe or effective operation of the school, or raises a safeguarding or behaviour concern.
- I understand that access to online content through school devices and systems is appropriately filtered and that use of school-provided devices, accounts and systems may be monitored, including when they are used away from the setting. The school can provide information about its filtering and monitoring arrangements.
- I understand that filtering and monitoring arrangements help to keep children safe, protect systems and support compliance with relevant policies, but cannot remove every online risk. Monitoring will be proportionate and undertaken in accordance with data protection, privacy and human rights requirements.

- I am aware of the school's expectations concerning mobile phones and smart devices and will support my child to follow them. If my child may need an exception or reasonable adjustment because of a disability, medical condition, communication need or other individual circumstance, I will discuss this with the school so that appropriate arrangements can be considered, agreed and recorded. I will support any individual arrangements agreed for my child. If I need to contact my child during the school day, I will use the school office or another agreed contact route, unless an alternative arrangement has been agreed.
- I will support my child to understand and follow the school's expectations for technology use, including social media, mobile phones, online communication, images and recordings and, where relevant, artificial intelligence tools.
- I will model safe, positive and respectful online behaviour and support my child not to create, post or share content that identifies, targets, threatens, bullies, harasses or risks causing harm to a child, family, member of staff or another member of the school community.
- If I have a concern or complaint, I am encouraged to use the school's established communication, safeguarding or complaints routes, as appropriate, so that it can be properly considered.
- I will report concerns about my child's online safety, or online concerns that may affect the safety or wellbeing of another member of the school community, to an appropriate member of staff. This may include Head of Year, the Designated Safeguarding Lead or Headteacher. Where necessary, I may also report the concern to another relevant organisation.
- If the school has concerns about my child's online safety or behaviour, I understand that these will be considered fairly and proportionately in line with relevant safeguarding, behaviour and other procedures. The school will communicate with me where it is appropriate and safe to do so.
- I understand my role in helping my child to use technology safely. As appropriate to my child's age, understanding and needs, I will consider the use of parental controls, provide suitable supervision and support, and encourage safe and responsible use of the internet and other technology at home.
- I know that I can seek online safety information or support from the school.

3. Letter for Parents/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/online-safety
- 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

4. Student & Parent/Carer Agreement Slip

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 bring my own devices into school, including mobile phones, smart technology, gaming devices, cameras or any device that can send or receive messages or notifications, or record audio, images or video.
- I use my own systems or 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 or when accessing school systems such as emails, Google suite or other educational platforms the school provides.

Name: Signed:.....

Class:..... Date:

Parent / Carers Name:

Parent/Carers Signature:

5. Staff, Trustee, Visitor & Volunteer Acceptable Use Policy Agreement

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use technology in a professional, lawful, and ethical manner.

This Staff, Trustee, Visitor & Volunteer Acceptable Use of Technology Policy (AUP) sets out Borden Grammar School's expectations for safe technology use, professional conduct, safeguarding, data protection and system security. It is not intended to unduly limit appropriate teaching, learning or professional use of technology, but to help protect pupils/students, staff, systems and the wider community from accidental or deliberate misuse.

All staff are asked to read, understand and sign this AUP.

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.
- It also applies to personal use of technology where this is linked to my role, involves the school community, uses school systems or information, could affect safeguarding, professional boundaries, confidentiality or data protection, or could reasonably impact on my professional role or the reputation of the school.
- 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 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.

Use of School Devices and Systems

- I will use school provided or approved equipment, systems and internet services when working with pupils, unless otherwise formally agreed by leaders.
- I understand that school equipment, systems and internet services are provided for education and/or professional use. Reasonable personal use is not permitted and, where allowed, must not interfere with my work duties, system security, safeguarding, confidentiality or professional boundaries. This permission is at the school's discretion and may be withdrawn at any time.
- Where I deliver or support remote learning, I will comply with the school's remote learning AUP.

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 follow the school's requirements for secure passwords, authentication and account access. I will keep authentication information secure and will not share passwords, verification codes or access credentials with others.
- 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 take care before opening links or attachments, including those apparently sent by a known

contact. I will check unexpected or suspicious messages through an appropriate route and report suspected phishing or malicious content to the IT Department.

- 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 only process or share personal data through school approved systems and services and in line with the setting's data protection and information-security procedures. Any proposed new or changed use of cloud services, AI tools or other online systems involving personal data will be risk assessed and approved through the setting's agreed process before use. Where required, a Data Protection Impact Assessment will be completed.
- 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 devices 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 Coordinator (Kirsty Murphy) as soon as possible.
- I will follow the school image use policy when taking, using, storing or sharing images or recordings of pupils. Images and recordings must always be appropriate and must only be taken using school provided or approved equipment. I will not use personal devices, including personal mobile phones, cameras, tablets, smart watches or other wearable technology, to take images or recordings of pupils. Images and recordings will only be taken, used or shared in line with the school image use policy, safeguarding expectations, data protection requirements and consent/lawful basis arrangements.

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 I become aware of a filtering or monitoring failure, or witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL and IT provider/staff, in line with the school's Safeguarding & Child Protection Policy.
- I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces, including the use of approved platforms, search tools and AI tools, as listed in the Child protection, online safety and remote learning acceptable use policy.
- I will follow the school's agreed approach to screen use. Any use of screens, devices, apps or online

content will be planned, purposeful, age appropriate and supervised, and will not replace face-to-face interaction, play, physical activity, rest, care routines or real-world exploration.

- I am aware that generative artificial intelligence (AI) tools may have many uses which could benefit our school community. However, I recognise that AI tools can also pose risks, including, but not limited to, bullying and harassment, abuse and exploitation (including child sexual abuse), privacy and data protection risks, plagiarism and cheating, and inaccurate, harmful and/or biased material. Additionally, their use can pose moral, ethical and legal concerns if not carefully managed. As such, I understand that:
 - AI tools must only be used responsibly, ethically and where the tool, purpose and use have been approved by leaders. Any new, unapproved or changed use of AI tools will be risk assessed and approved before use, in line with child protection, data protection and professional conduct expectations.
 - I understand that AI-generated content must be checked for accuracy, bias, appropriateness, copyright and safeguarding implications before it is used or shared.
 - I will not enter personal, sensitive, confidential, safeguarding, assessment or special category information, or images of pupils, staff or other identifiable individuals, into any AI tool unless the tool has been approved for that purpose, the use has been risk assessed, consent has been obtained where required, and the DPO/leadership team has confirmed that the processing is lawful and appropriate.
 - I will not add or use AI note takers, transcription tools, recording bots or automated meeting summary tools in any meeting, lesson, supervision, training or professional discussion unless this has been agreed in advance by leadership. Where approved, I will ensure that participants are made aware and their use is transparent, proportionate and in line with safeguarding, confidentiality, consent, data protection and information governance expectations.
 - I will not use AI to make decisions about pupils, families or staff, including decisions relating to safeguarding, behaviour, SEND, assessment, attendance, admissions, recruitment, allegations or pastoral support, without appropriate professional oversight and in line with setting policy.
 - Only approved AI platforms may be used with pupils. Pupils must be supervised when using AI tools, and I must ensure age-appropriate use and understanding prior to use.
 - I will report any concern involving AI misuse, including deepfake or manipulated content, impersonation, harmful AI-generated material, AI-facilitated bullying or harassment, or AI-generated nude/semi-nude imagery, in line with the school child protection, behaviour, anti-bullying, staff conduct and data protection procedures.
- 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, Tim Westby, 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 are 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.

Use of Social Media and Mobile Technology

- I will ensure that my use of mobile devices and smart devices 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, the Staff Code of Conduct and the school mobile technology policy and the law.
- I will model safe and professional use of mobile phones and smart devices and will support the school's expectations for pupils.
- Where mobile phones or smart devices are used for professional purposes, such as authentication, learning activities, recording rewards or sanctions, or other agreed tasks, I will use school provided devices where available. Where staff are permitted to use personal devices for professional purposes, this must be formally agreed by the school and managed in line with school policy.
- Any use of a personal mobile phone or smart device for professional purposes, or in exceptional circumstances, must be transparent, necessary, proportionate and approved by the headteacher or other designated leader. Use must not compromise supervision, safeguarding, confidentiality, professional boundaries, data protection or the learning environment.

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.
- I will protect myself, my professional reputation and the reputation of the school online. I will not discuss or share data or information relating to pupils, staff, school business or parents/carers on social media.
- My electronic communications with current and former pupils 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-provided communication channels and systems, such as a school email address, user account or telephone number.
- I will not use personal accounts, personal profiles, personal phone numbers, private messaging apps, gaming accounts or other personal communication channels to contact or communicate with pupils or their families, unless this has been formally approved, risk assessed and recorded by leaders.
- I will not share any personal contact information or details with pupils, such as my personal address, email address or phone number.
- I will not share personal information about my private life with pupils online, through messaging, social media, gaming platforms, apps or other digital communication channels. I will maintain appropriate professional boundaries in all digital communication.
- I will not add, follow, accept or respond to friend requests, direct messages or other personal online communication from current or former pupils, or their parents/carers, where this is linked to my role, the school, or could blur professional boundaries. Any attempted contact will be reported to my line manager and/or the DSL.
- Any pre-existing links, relationships or situations that affect how I apply the AUP or other relevant policies will be discussed with the DSL and/or headteacher. This is to help safeguard pupils, staff and the wider school community by ensuring professional boundaries, safeguarding expectations and communication arrangements are clear.
- Where digital communication with pupils or families is required, I will follow the school's expectations about when communication should take place, including any agreed arrangements for out-of-hours

contact, emergency communication or role-specific responsibilities.

Policy Concerns

- I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, terrorist material or adult pornography covered by the Obscene Publications Act.
- I will not access, create, transmit, display, publish, forward, discuss, send, share or show any material or content that may be harmful, inappropriate, adult, offensive, unprofessional, or likely to harass, cause offence, inconvenience or needless anxiety to any other person. This applies when using school systems, school devices, personal devices, personal accounts, messaging apps, online platforms, social media or shared spaces. It includes content shared in staff rooms, offices, online groups or other staff communication spaces, where this takes place on school premises, during working time, or in any context linked to my role.
- I will not engage in online or digital behaviour linked to my role that compromises safeguarding, professional boundaries, confidentiality, data protection, public confidence in my professional conduct or my ability to carry out my role.
- 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, conduct, or behaviour of staff, including online, digital, device-related or technology-linked concerns, to the Headteacher, in line with the school child protection policy, staff behaviour policy/code of conduct, low-level concerns procedures and/or allegations against staff policy.

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 and information systems to check 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.
- Staff will be informed about the nature, purpose and extent of monitoring through this AUP, relevant policies, privacy information and/or staff guidance.
- 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.
- If I find myself in a situation where my online contact, device use, recording, image use or AI use could be misinterpreted, I will report this promptly to the DSL and/or Headteacher so it can be recorded and managed transparently.
- Any breach or concern involving online contact, device use, images, recordings, social media, AI use, confidentiality, data protection or professional boundaries must be reported to the Headteacher and/or DSL without delay, even if it appears minor, accidental or unlikely to meet the harm threshold.
- I understand that if the school believes that unprofessional or inappropriate online or technology-related activity may have compromised safeguarding, professional boundaries, confidentiality, data protection, public confidence in professional conduct or my ability to carry out my role, the concern will be considered fairly, proportionately and confidentially, in line with relevant safeguarding, staff behaviour, low-level concerns, allegations, data protection and disciplinary procedures. Where the concern may meet the harm threshold, advice will be sought and/or a referral

made to the Local Authority Designated Officer (LADO) in line with local allegations procedures. Where it does not meet this threshold, it will still be recorded and responded to appropriately.

- Where a concern involves personal data, confidential information, safeguarding information, images, recordings, AI tools, transcription tools or unauthorised sharing, the DPO/data protection lead will be informed promptly so that any data protection, information governance or reporting requirements can be considered.
- I understand that if the school suspects criminal offences have occurred, the police will be informed where appropriate.
- I understand that this AUP cannot cover every possible situation. If I am unsure whether any use of technology, online communication, image use, recording, personal device use, social media, AI tool or digital contact is appropriate, I will seek advice from the DSL and/or Headteacher before taking action. I will act in a way that safeguards [children/pupils/students], protects professional boundaries, and is open to scrutiny.

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 (DD/MM/YY):