



# Online Safety Policy

Review Responsibility:	Assistant Headteacher – Safeguarding & Inclusion
Frequency of Review:	1 year
Date Approved:	Sep 25
Approved By:	Board of Trustees
Next Review Due By:	Sep 26

# Contents

<b>1. Aims</b>	<b>3</b>
<b>2. Legislation and Guidance</b>	<b>3</b>
<b>3. Roles and Responsibilities</b>	<b>3</b>
3.1 The Trustees	3
3.2 The Headteacher	4
3.3 The Designated Safeguarding Lead (DSL)	4
3.4 The ICT Manager	5
3.5 All Staff and Volunteers	5
3.6 Parents/Carers	6
3.7 Visitors and Members of the Community	6
<b>4. Educating Pupils about Online Safety</b>	<b>6</b>
<b>5. Educating Parents/Carers about Online Safety</b>	<b>7</b>
<b>6. Cyberbullying</b>	<b>7</b>
6.1 Definition	7
6.2 Preventing and addressing cyber-bullying	7
6.3 Examining electronic devices	8
6.4 Artificial Intelligence (AI)	9
<b>7. Acceptable Use of the Internet in School</b>	<b>9</b>
<b>8. Pupils Using Mobile Devices in School</b>	<b>9</b>
<b>9. Staff Using Work Devices Outside School</b>	<b>10</b>
<b>10. How the School will Respond to Issues of Misuse</b>	<b>10</b>
<b>11. Training</b>	<b>10</b>
11.1 Staff, trustees and volunteers	10
11.2 Pupils	11
<b>12. Monitoring Arrangements</b>	<b>11</b>
<b>13. Links with Other Policies</b>	<b>11</b>
<b>Appendix 1 – Student Acceptable Use Policy Agreement</b>	<b>13</b>
<b>Appendix 2 – Staff, Trustee, Visitor and Volunteer Acceptable Use Policy Agreement</b>	<b>16</b>

## 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, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, 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 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](#)
- [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](#)

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](#) 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 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 will regularly review their effectiveness. 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.

### **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 about 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](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education \(for teaching until 31 August 2026\)](#).

**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
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed 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
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.

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.

## 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

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 and 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. They can carry out a search and confiscate any electronic device 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), they will:

- **Not** view the image

- 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](#)

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 / searches and 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 Bard.

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.

## **8. Pupils Using Mobile Devices in School**

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

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 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 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

### 11.1 Staff, trustees and 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, especially around chat groups
  - Sharing of abusive images and pornography, 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.

## 11.2 Pupils

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 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 training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

## 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:

- Child protection and safeguarding policy
- Behaviour policy

- Staff disciplinary procedures
- UK GDPR and Data protection policy and privacy notices
- Complaints policy and procedure
- ICT and internet acceptable use policy
- Anti-bullying Policy
- Whistleblowing Policy
- Searching Screening and Confiscation Policy
- RSE Policy

# Appendix 1 – Student Acceptable Use Policy Agreement

## 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

### 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. 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.

### **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.

### **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](http://www.thinkuknow.co.uk) [www.childnet.com](http://www.childnet.com) and [www.childline.org.uk](http://www.childline.org.uk) to find out more about keeping safe online
- I have read and talked about these rules with my parents/carers

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 device 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: .....

# Appendix 2 – Staff, Trustee, Visitor and Volunteer Acceptable Use Policy Agreement

## 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 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 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.

### **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.

- o 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.
- o 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.
- o 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.
- o 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:
  - o 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
  - o 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.
  - o 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.
  - o I will not share any personal contact information or details with students, such as my personal email address or phone number.
  - o I will not add or accept friend requests or communications on personal social media with current or past students and/or their parents/carers.
  - o 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).
  - o 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 (DD/MM/YY): .....