Online Safety Policy

RIDGEWAY EDUCATION TRUST

Approved by the Trust Board: March 2025
Review date: March 2026

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- 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, fake news, 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
- 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 Trust Board

The Trust board has overall responsibility for monitoring this policy and holding the CEO and headteachers of Ridgeway Education Trust (RET) schools to account for its implementation.

The Trust board 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 Trust board 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 Trust board, through the Trustee appointed for Safeguarding and the Local Governing Body Safeguarding Link Governor, 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 Trust board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust board must ensure 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 schools in meeting those 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 Appointed Safeguarding Lead who oversees online safety is Andrew Kaye.

All Trustees and governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- 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, vITims 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

3.3 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.4 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in the schools 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 local governing body 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
- Working with the RET IT Services Lead to make sure the appropriate systems and processes are in place
- Working with the headteacher, RET IT Services Lead 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
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Trust board
- Where appropriate, undertaking annual risk assessments that consider and reflect the risks children face in line with our acceptable use policy.
- 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
- The DSL will provide a report to the local governing bodies and Trust Board at least three times annually, or when requested.

This list is not intended to be exhaustive.

3.5 RET IT Strategy Forum

The IT Strategy Forum and the Security and Compliance sub-committee is responsible for

- Setting the strategic direction of IT security across the trust/school(s), including the development and oversight of online safety and cybersecurity measures.
- Evaluating and approving key decisions regarding the implementation of security systems, software, and protocols designed to protect users, data, and infrastructure
- Ensuring that security protection decisions align with current legislation, best practice guidance (e.g., DfE, NCSC), and the trust's risk management strategy.
- Reviewing incidents, trends, and threat intelligence to inform ongoing improvements to security policies and systems.
- Providing guidance to schools on adopting safe digital practices and ensures consistency of security standards across all sites within the trust.

3.6 The RET Chief Operating Officer

The Chief Operating Officer (COO) is responsible for

- Determining and approving the operational procedures for IT security protection across the trust/school(s), in line with strategic direction set by the IT Strategy Forum.
- Working in collaboration with the IT Services Lead to ensure that appropriate and effective security protection procedures are developed, implemented, and maintained.
- Together with the IT Services Lead, assesses risks, identifies priorities, and ensures that security measures are proportionate, cost-effective, and responsive to emerging threats
- Overseeing the communication and enforcement of security procedures, ensuring that staff, students, and stakeholders are aware of their responsibilities.
- Monitoring, alongside the IT services Lead, the effectiveness of security procedures and ensures regular review cycles, including updates following incidents, audits, or changes in risk levels.
- Supporting the allocation of resources (financial, technical, and human) necessary to implement and sustain robust security protection measure including the procurement and deployment of firewalls, filtering systems, antivirus solutions, and endpoint protection tools.

3.7 The RET IT Services Lead

The RET IT Services Lead 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 the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting regular audits of the IT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged 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.

3.8 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 IT systems and the Internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 through the RET IT Services helpdesk.
- Following the correct procedures by seeking approval through the IT Service Desk and RET DSL if they need to make exceptions to the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

3.9 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 IT systems and Internet (appendices 1 and 2), as applicable).

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
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.10 Visitors and Members of the Community

Visitors and members of the community who use the school's IT systems or Internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, 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 **Key Stage 4** 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 which 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 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, for example, letters or other communications home, and in information via our websites.

Online safety will also be covered during parents' evenings where appropriate and applicable.

If requested, the schools will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being required 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. Cyber-bullying

6.1 Definition

Cyber-bullying 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the schools' behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, 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 schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. As part of the Personal Development curriculum cyber bullying awareness will be taught which provides sensible guidance for students of how to keep safe and happy on the Internet.

All staff, governors 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 cyber-bullying 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 cyber-bullying, the schools will follow the processes set out in the schools' behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the schools 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, and any member of staff authorised to do so by the headteacher (as set out in the schools' behaviour policy, 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 headteacher / DSL / appropriate staff member
- 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 the staff member in conjunction with the DSL / headteacher / other member of the senior 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
- The school's behaviour 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.

Ridgeway Education Trust 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 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Ridgeway Education Trust will treat any use of AI to bully pupils in line with our 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/trust.

7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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, governors 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 to 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school but are not permitted to use them during the school day (including break times) unless in exceptional circumstances and by prior authorisation by a member of staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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 school/trust issued devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device is locked if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems and anti-virus 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 3.

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 RET IT Services.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or Internet, we will follow the procedures set out in our policies on behaviour and IT acceptable use. 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 IT systems or the Internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the RET Disciplinary Procedure and Safeguarding Code of Conduct. The action taken will depend on the circumstances, nature and seriousness of the specific incident.

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

12. Training

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 and staff briefings).

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, 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 deputy/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.

Governors 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.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMS.

This policy will be reviewed every year by the RET Safeguarding Lead and IT Services Lead. At every review, the policy will be shared with the Trust Board. The review will be supported by an annual risk assessment 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.

Prior to approval and ratification, the policy will be shared with the RET CEO and RET COO.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT acceptable use policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's IT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school IT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's IT systems (like computers) and get onto the** Internet **in school I will:** • Always use the school's IT systems and the Internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's systems using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:
When using the school's IT systems and accessing the Internet **in school, or outside school on a work device (if applicable), I will not:** • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
I will only use the school's IT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's IT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and RET IT Services Lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's IT systems and Internet responsibly, and ensure that pupils in my care do so too.

Appendix 4: Use of Personally Owned Devices (BYOD) Agreement

Use of Personally Owned Devices (BYOD) Agreement

Purpose: This agreement outlines the responsibilities and acceptable use of personally owned devices by staff members at Ridgeway Education Trust. The aim is to ensure that staff use their devices in a manner that is secure, responsible, and compliant with school policies, particularly when storing school-related data.

Scope: This agreement applies to all staff members, including teachers, administrative staff, trustees, governors, and volunteers, who wish to store school-related data on their personally owned devices (such as laptops, tablets, and smartphones).

Responsibilities:

1. **Device Security and Safety:**
   - Staff are responsible for the security and safety of their devices at all times.
   - Devices should be password-protected and have up-to-date antivirus software installed.
   - The trust/school is not liable for any loss, theft, or damage to personal devices.
   - **It is recommended to enable "Find My Device" or a similar feature if available on the BYOD**. This can help locate the device if it is lost or stolen and ensure that data can be remotely wiped if necessary.
2. **Acceptable Use:**
   - Devices should be used for work-related purposes only during school hours.
   - Staff must adhere to the trust/school's IT Acceptable Use Agreement and Online Safety Policy.
   - Accessing inappropriate content, including but not limited to violent, pornographic, or offensive material, is strictly prohibited.
   - Staff must not use their devices to bully, harass, or intimidate others.
3. **Network Access:**
   - Staff may connect their devices to the school's Wi-Fi network for work-related purposes.
   - The use of personal data plans or personal VPNs to bypass the school's network restrictions when using BYODs for educational purposes is not allowed.
   - The school/trust reserves the right to monitor network activity on devices connected to its systems and restrict access to certain websites and services.
4. **Privacy and Data Protection:**
   - Staff must respect the privacy of others and not access, modify, or share data without permission.
   - Personal data related to school activities should be stored securely and deleted when no longer needed.
   - Staff should not share their device passwords with others.
   - Sensitive school-related information stored or synced on BYODs must be protected with a password or PIN. **Encryption should be enabled (where possible) to further secure the data**.
   - **It is recommended that that the staff member create a separate password-protected profile on their device, if possible, to ensure that school-related data is not confused with personal data.**
5. **Compliance and Consequences:**
   - Any breach of this agreement may result in disciplinary action, including but not limited to the loss of BYOD privileges.
   - Serious violations may be reported to the appropriate authorities.

Agreement: By signing this agreement, staff members acknowledge that they have read, understood, and agree to abide by the terms and conditions outlined above.

Signed (staff member/governor/volunteer/visitor):	**Date**

Appendix 5: Use of Personally Owned Equipment by Sixth Form Students (BYOD) Agreement

Use of Personally Owned Equipment by Sixth Form Students (BYOD) Agreement	
Name of pupil:	
Purpose: This agreement outlines the responsibilities and acceptable use of personally owned devices by Sixth Form students at Ridgeway Education Trust. The aim is to ensure that students use their devices in a manner that is safe, responsible, and conducive to their education. **Scope:** This agreement applies to all Sixth Form students who wish to use their personally owned devices (such as laptops, tablets, and smartphones) within the school premises. **Responsibilities:** **1. Device Security and Safety:** • Students are responsible for the security and safety of their devices at all times. • Devices should be password-protected and have up-to-date antivirus software installed. • The school is not liable for any loss, theft, or damage to personal devices. • **It is recommended to enable "Find my Device" or a similar feature if available on the BYOD.** This can help locate the device if it is lost or stolen. **2. Acceptable Use:** • Devices should be used for educational purposes only during school hours. • Students must adhere to the school's IT Acceptable Use Agreement and Online Safety Policy. • Accessing inappropriate content, including but not limited to violent, pornographic, or offensive material, is strictly prohibited. • Students must not use their devices to bully, harass, or intimidate others. **3. Network Access:** • Students may connect their devices to the school's Wi-Fi network for educational purposes. • The use of personal data plans to bypass the school's network restrictions is not allowed. • The school reserves the right to monitor network activity and restrict access to certain websites and services. **4. Privacy and Data Protection:** • Students must respect the privacy of others and not access, modify, or share data without permission. • Personal data related to school activities should be stored securely and deleted when no longer needed. • Students should not share their device passwords with others. **5. Compliance and Consequences:** • Any breach of this agreement may result in disciplinary action, including but not limited to the confiscation of the device and loss of BYOD privileges. • Serious violations may be reported to the appropriate authorities. **Agreement:** By signing this agreement, students and their parents/carers acknowledge that they have read, understood, and agree to abide by the terms and conditions outlined above.	
Signed (Student):	**Date**

Appendix 6 – Device Loan Agreement

Ridgeway Education Trust: Device Loan Agreement

This device and any accessories detailed below have been loaned to you to support your work in RET or in one of the schools forming part of the Trust (RET, the Trust, the School). The device is intended for use in assisting the delivery of the curriculum and other work-related activities.

This loan is subject to the terms and conditions listed below. Failure to adhere to these terms may result in the loan being terminated early, and/or other consequences as outlined in this agreement.

The loan and accompanying terms and conditions are subject to review and amendment on a regular basis and can be withdrawn at any time.

Duration of Loan

The loan period will begin on the date you sign this agreement and will be reviewed at least annually. An expected return date may be issued along with this agreement. The borrower agrees to return the device and all accessories listed in this agreement to RET IT Services either:

- By the end of the loan period.
- When requested by RET IT Services.
- Upon termination of employment by the Trust or the Schools making up the Trust.

Loan Terms and Conditions

By accepting this loan, the borrower agrees to the following terms and conditions:

1. The device and accessories provided with it remain the property of the Trust and are strictly for the borrower's sole use in assisting the delivery of the curriculum and other work-related activities.

2. The borrower agrees to treat the device with due care and keep the device in good condition, not leave the device unattended in a room (e.g. classroom or office) without being secured, and avoid food and drink near the device.

3. The borrower not to place any stickers, labels or other adhesive materials on the device or any of its accessories without prior written consent from the Trust.

4. RET IT Services regularly backs up data saved to the Trust computer network, and the borrower accepts responsibility for backing up any data saved only on the device.

5. The borrower agrees to only use software licensed by the Trust, authorised by the IT Services Lead, and installed by RET IT Services.

6. The borrower understands that any anti-virus software that is installed must be updated on a regular basis.

7. The borrower agrees to follow all policies and restrictions on the device that are in place to protect the Trust's Networks, and not to circumvent or disable these restrictions.

8. Should any faults occur, the borrower agrees to notify RET IT Services as soon as possible, so that they may undertake any necessary repairs. Under no circumstances should the borrower or anyone other than RET IT Services attempt to fix suspected hardware or any other faults.
    i.

9. The borrower understands that if the device becomes broken beyond economical repair whilst in their care during the loan period, they or their department may be responsible for funding either in whole or in part a replacement device as specified by RET IT Services.
    ii. It is recommended that the borrower has personal possession insurance that will cover devices loaned to them by RET.

10. Some devices may include accidental damage protection, which allows up to one claim per device, per year. You should enquire about such cover for further details on how to make a claim.

11. The borrower agrees that home Internet access is permitted at the discretion of RET IT Services. RET IT Services will not accept responsibility for offering technical support relating to home Internet connectivity, or devices not owned by RET.

12. The borrower agrees that any telephone/broadband charges incurred when accessing the Internet from any site other than RET premises are not chargeable to the Trust.

13. The borrower agrees to adhere to School and Trust policies, including but not limited to:
    i. Acceptable Use
    ii. GDPR and Data Protection
    iii. Health and Safety
    iv. Keeping Children Safe in Education

14. The borrower understands that RET IT Services may need to perform maintenance on the device and agrees to return the device when requested for this to happen. RET IT Services will give reasonable notice of any planned or unplanned maintenance that must be performed on the device.

15. Should the device become lost or stolen, the borrower will inform RET IT Services and gdpr@ridgewayeducation.com as soon as possible after becoming aware of the incident.

16. The borrower understands that failure to return the device and all accessories listed in this agreement at the end of the loan period or upon termination of employment will result in them being responsible for making payment towards the cost of replacing those such items. By agreeing to these terms, the borrower consents to any such payments being made through deductions from their salary, or from outstanding payments owed to them.