Online Safety Policy 2023-24

Part One : **Safe use of mobile and smart technology expectations**

Part Two : Monitoring and Filtering Systems

Part Two: **Social Media**

Part Three: **Acceptable Use of Technology including remote learning**

Part One

Safe use of mobile and smart technology expectations

1. Policy aims and scope

- This policy has been written by Rodmersham School, involving staff, learners and parents/carers, , taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, Early Years and Foundation Stage 2021 (***if applicable***) 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of the Rodmersham School community when using mobile devices and smart technology.
  - Rodmersham School recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using mobile and smart technology.
  - As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), *Nicky McMullon, Headteacher* is recognised as having overall responsibility for online safety.
- This policy applies to all access to and use of all mobile and smart technology on site; this includes mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as 'smart watches and fitness trackers, which facilitate communication or have the capability to record sound or images.
- This policy applies to learners, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

- It is essential that children are safeguarded from potentially harmful and inappropriate material or behaviours online. Rodmersham will adopt a whole school approach to online safety which will empower, protect, and educate our pupils and staff in their use of technology, and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate.
- Rodmersham will ensure online safety is considered as a running and interrelated theme when devising and implementing our policies and procedures, and when planning our curriculum, staff training, the role and responsibilities of the DSL and parental engagement.
- Rodmersham identifies that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
  - Content: being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
  - Contact: being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
  - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- Rodmersham recognises that technology and the risks and harms related to it evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment, which considers and reflects the current risks our children face online.
- The headteacher will be informed of any online safety concerns by the DDSL, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

2. Links with other policies

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Child protection policy
    - Code of conduct
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data security

3. Safe use of mobile and smart technology expectations

- Rodmersham School recognises that use of mobile and smart technologies is part of everyday life for many learners, staff and parents/carers.
- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the Rodmersham School community are advised to:
    - take steps to protect their mobile phones or personal devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.
- Mobile phones and personal devices are not permitted to be used in specific areas on site, such as the toilets or communal staff areas.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, Code of Conduct and child protection policies.
- All members of the Rodmersham School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our Code of Conduct or child protection policies.

4. Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant *school* policy and procedures, such as confidentiality, child protection, data security and Code of Conduct Policy.

- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods unless written permission has been given by the *headteacher*, such as in emergency circumstances.
  - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers without permission from the SLT. In the case of emergency staff must use 141 at the start of the phone number.
  - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL/*headteacher.*
- Staff will only use *school* provided equipment (not personal devices):
  - to take photos or videos of learners in line with our image use policy.
  - to work directly with learners during lessons/educational activities.
  - to communicate with parents/carers.
- Where remote learning activities take place, staff will use *school* provided equipment. If this is not available, staff will only use personal devices with prior approval from the *headteacher,* following a formal risk assessment. Staff will follow clear guidance outlined in in this policy in line with Acceptable Use
- If a member of staff breaches our policy, action will be taken in line with our staff *code of conduct* and allegations policy.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.
-

5. Learners use of mobile and smart technology

- Learners will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.
- Safe and appropriate use of mobile and smart technology will be taught to learners as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection.
- Mobile phones and/or personal devices *will* not be used on site by learners.

- Rodmersham School expects learners' personal devices and mobile phones to be kept safe and secure when on site. This means:
  - ***Handing it to a member of staff to be kept in a secure place until the end of the day.***
- If a learner needs to contact their parents or carers whilst on site, the staff member will contact them on their behalf via the office.
  - Parents are advised to contact their child via the *school* office.
- If a learner requires access to a personal device in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the *headteacher* prior to use being permitted.
  - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the *school.*
- Where learners' mobile phones or personal devices are used when learning at home, this will be in accordance with *Acceptable Use part of this document.*
- Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, child protection and behaviour.

6. Visitors' use of mobile and smart technology

Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

- They understand that any activity on a school device or using school networks/platforms/internet may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
- They will leave their phone in their pocket and turned off. Under no circumstances will they use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), they will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- If they are given access to school-owned devices, networks, cloud platforms or other technology:
  - They will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
  - They will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of their role
  - They will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
  - They will protect their user name/password and notify the school of any concerns
  - They will abide by the terms of the school Data Protection Policy

    - They will not share any information about the school or members of its community that they gain as a result of their visit in any way or on any platform except where relevant to the purpose of their visit and agreed in advance with the school.
    - They will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
    - They will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils/students and will not give any advice on online-safety issues unless this is the purpose of their visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).
    - They will only use any technology during their visit, whether provided by the school or their personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to their visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

- Appropriate signage and information is in place with a leaflet which is handed out to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.
- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use policy and other associated policies, including child protection.
- If visitors require access to mobile and smart technology, for example when working with learners as part of multiagency.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or *headteacher* of any breaches of our policy.

7. Policy monitoring and review

- Technology evolves and changes rapidly. Rodmersham School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

8. Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing *school* policies and procedures. This includes: ***Staff Code of Conduct and Child Protection Policies.***
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or *headteacher* will seek advice from the Education People's Education Safeguarding Service or other agency in accordance with our child protection policy.

Part Two – Monitoring and Filtering Systems

Appropriate filtering and monitoring on school devices and networks

- Rodmersham will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.

- When implementing appropriate filtering and monitoring, Rodmersham will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.
  - Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment.
  - Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm and they will always be supervised by an adult.

Responsibilities

- Our governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

- Emma Foord a member of the school staff and Alun Phillips governor, are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.
- Our headteacher is responsible for
  - procuring filtering and monitoring systems.
  - documenting decisions on what is blocked or allowed and why.
  - reviewing the effectiveness of our provision.

  - overseeing reports.
  - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
  - ensuring the DSL and staff have sufficient time and support to manage their filtering and monitoring responsibilities.

- The DSL has lead responsibility for overseeing and acting on:
  - any filtering and monitoring reports.
  - any child protection or safeguarding concerns identified.
  - checks to filtering and monitoring system.

- The staff have technical responsibility for:
  - maintaining filtering and monitoring systems.
  - providing filtering and monitoring reports.
  - completing technical actions identified following any concerns or checks to systems.
  - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.
- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our staff works closely with the DSL. Decisions will be recorded and informed by an approach which ensures our systems meet our school specific needs and circumstances, including but not limited to our pupil risk profile and specific technology use.

- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- Our school undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.
- In addition, our school undertakes regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the governing body that we are meeting our safeguarding obligations.
  - These checks are achieved by: List how this is achieved within your school for example weekly, monthly, termly checks are undertaken by a DSL, checks are undertaken with two members of staff present (it may be helpful to list who e.g. a DSL and a member of IT or SLT), checks are undertaken in a location where confidentiality can be achieved, during working hours, when pupils are not present (e.g. headteachers office), checks are

logged/recorded, any technical concerns are flagged to the IT staff/IT service provider and safeguarding concerns are actioned by the DSL etc.in line with this policy

Appropriate filtering

Settings should list specific details of how their appropriate filtering is established and achieved in their setting; for example, which filtering systems/approaches are in place and why these decisions have been made. Leaders and DSLs should access the UK Safer Internet Centre guidance and the DfE filtering and monitoring standards for further information about appropriate monitoring approaches and what they entail.

No filtering system can be 100% effective; schools and colleges need to understand the coverage of their filtering system, any limitations it has, and mitigate accordingly to minimise harm and meet their statutory requirements as identified in KCSIE and the Prevent duty.

- [Name of School/College]'s education broadband connectivity is provided through [name of internet service provider] and Rodmersham uses [name of filtering system].
  - [Internet Service Provider] is a member of Internet Watch Foundation (IWF). **Leaders should check to ensure this is the case.**
  - [Name of filtering system] has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) **Leaders should check to ensure this is the case.**
  - [Name of filtering system] is blocking access to illegal content including child sexual abuse material (CSAM).
  - [Name of filtering system] blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material. **Please note this list is not exhaustive and schools/colleges should amend this list as required and appropriate to leadership decisions.**

- We filter internet use on all school owned, or provided, internet enabled devices and networks. This is achieved by:
  - **Detail how this is achieved and explain what filtering is in place for all school provided devices and access to any school systems, including any offsite access.**
  - **This section should include any specific filtering approaches required for mobile devices such as tablets and eReaders, and any guest access to systems such as Wi-Fi, as the approaches for these systems may differ.**
  - **Filtering systems should allow school/colleges to identify device names or IDs, IP addresses, and where possible, individual users, the time and date of attempted access and the search term or content being blocked.**

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection. **Leaders should check to ensure this is the case.**

- We work with [name of internet service provider/filtering provider] and our IT service providers/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to:
  - Insert details of your procedure, for example, turn off monitor/screen, use a screen cover widget, report the concern immediately to a member of staff, report the URL of the site to technical staff/services.

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies. **Amend as appropriate.**

- Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.
- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

Appropriate monitoring

Settings should list specific details of how their appropriate monitoring approaches are established and achieved in their setting; for example, the monitoring systems/approaches in place and leaders should be able to explain why these decisions have been made. Leaders and DSLs should access the UK Safer Internet Centre guidance and the DfE filtering and monitoring standards for further information about appropriate monitoring approaches and what they entail.

No monitoring system can be 100% effective; schools and colleges need to understand the coverage of their monitoring approaches system, any limitations, and mitigate accordingly to minimise harm and meet their statutory requirements as identified in KCSIE and the Prevent duty.

- We will appropriately monitor internet use on all school provided devices and networks. This is achieved by:
  - **Detail how this will be achieved, for example, physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services. This should explain what monitoring is in place on all school provided devices and systems, including offsite access.**
  - **This section should include any specific monitoring approaches required for mobile devices such as tablets and eReaders and any guest access to Wi-Fi as the approaches for these systems may differ.**

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation. **Schools/colleges should link to any relevant policies and documents e.g., acceptable use or behaviour policies and privacy notices.**

- If a concern is identified via our monitoring approaches:
  - Where the concern relates to pupils/students, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies. **Amend as appropriate.**
  - Where the concern relates to staff, it will be reported to the headteacher (or chair of governors if the concern relates to the headteacher), in line with our staff behavior/ allegations policy. **Amend as appropriate.**

- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.

6.3 Information security and access management

- Rodmersham is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems as well as staff and pupils/students. Further information can be found in list name of relevant policies, for example, information security, acceptable use policies and/or online safety policy. **These policies should address expectations with regards information security and access to systems, for example password safety expectations.**
- Rodmersham will review the effectiveness of our procedures periodically to keep up with evolving cyber-crime technologies.
- Emma Foord a member of the teaching staff and Alun Philips governor, are responsible for ensuring that our school has met the DfE cyber security standards for schools and colleges. **Amend as appropriate. KCSIE 2023 states that schools and colleges should consider meeting the DfE Cyber security standards for schools and colleges.**

6.4 Remote/Online learning

Specific guidance for DSLs and SLT regarding remote learning is available at

- **DfE: Safeguarding and remote education during coronavirus (COVID-19)**
- **NSPCC: Undertaking remote teaching safely**
- **The Education People: Remote Learning Guidance for SLT**

- Rodmersham will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and any local/national guidance.

- All communication with pupils and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems: Google Classroom, Microsoft 365 or equivalent.
  - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

- Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy/code of conduct and Acceptable Use Policies. **Amend as appropriate.**

- Staff and pupils will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP). **A template remote learning AUP for schools/colleges to adapt is available here. If schools/colleges do not have a sperate remote learning AUP, key messages and expectations should be included within this policy or added to existing AUPs.**

6.5 Online Safety Training for Staff

- Rodmersham will ensure that all staff receive online safety training, which, amongst other things, will include providing them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring, as part of induction.

- Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach. See section 7 for more information.

6.6 Educating pupils

- Rodmersham will ensure a comprehensive whole school curriculum response is in place to enable all pupils to learn about and manage online risks effectively as part of providing a broad and balanced curriculum. See section 9 for more information.

DSLs and leaders may find it helpful to access UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance. A variety of online safety templates and guidance from the Education Safeguarding Service can be accessed here.

6.7 Working with parents/carers

- Rodmersham will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential benefits and risks and to reinforce the importance of children being safe online by:

  - Include details here; for example, providing information on our school website and through existing communication channels (such as official social media, newsletters), offering specific online safety events for parents/carers or highlighting online safety at existing events.

- Rodmersham will ensure parents and carers understand what systems are used to filter and monitor their children's online use at school/college, 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 is going to be interacting with online. This is achieved by:
  - Include details here. For example, providing information on our school website and relevant policies such as acceptable use, home/school agreements and through existing communication channels.

- Where the School is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response. **Additional local advice and support is available for DSLs and SLT via the Education Safeguarding Service and our ' Think before you scare' blog post.**
-

6.1 Policies and procedures

- The DSL has overall responsibility for online safety within the school but

- The DSL will respond to online safety concerns in line with our child protection and other associated policies, including our Anti-bullying policy, Social Media policy and behaviour policies.

  - Internal sanctions and/or support will be implemented as appropriate.
  - Where necessary, concerns will be escalated and reported to relevant partner agencies in line with local policies and procedures.

- Rodmersham uses a wide range of technology. This includes: computers, laptops, tablets and other digital devices, the internet, our learning platform, intranet and email systems.
  - All school owned devices and systems will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- Rodmersham recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras, wearable technology and any other electronic devices with imaging and/or sharing capabilities. In accordance with KCSIE and EYFS:
  - Rodmersham has appropriate mobile and smart technology and image use policies in place, which are shared and understood by all members of the community. These policies can be found on the staff shared TEAMS.

Part Three

Social Media

1. Policy aims and scope

- This policy has been written by Rodmersham School, involving staff, learners and parents/carers, , taking into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, Early Years and Foundation Stage 2021 (***if applicable***) 'Working Together to Safeguard Children' 2018 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of Rodmersham School community when using social media.
  - *Rodmersham School* recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm when using social media.
  - As outlined in our child protection policy, the Designated Safeguarding Lead (DSL), *Nicky McMullon, Head Teacher* is recognised as having overall responsibility for online safety.
- The policy applies to all use of social media; the term social media includes, but is not limited to, blogs, wikis, social networking sites, forums, bulletin boards, online gaming, apps, video/photo sharing sites, chatrooms and instant messenger apps or other online communication services.
- This policy applies to learners, parents/carers and all staff, including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

2. Links with other policies

- This policy links with several other policies, practices and action plans, including but not limited to:*.*
  - Anti-bullying policy
  - Staff Code of Conduct policy
  - Child protection policy
  - Confidentiality policy
  - Personal Social and Health Education (PSHE) Policy
  - Data security

3. General social media expectations

- All members of the Rodmersham School community are expected to engage in social media in a positive and responsible manner.

- All members of the Rodmersham School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media whilst using *school* provided devices and systems on site by using the most appropriate monitoring and filtering systems.
- Inappropriate or excessive use of social media during *school* hours or whilst using *school* devices may result in removal of internet access and/or disciplinary action.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL and/or *headteacher* prior to use. Any use will take place in accordance within the acceptable use element of this policy.
- Concerns regarding the online conduct of any member of Rodmersham School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff code of conduct and child protection.

4. Staff use of social media

- The use of social media during *school* hours for personal use *is not* permitted for staff.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our *code of conduct and acceptable use of technology as outlined in this policy.*
- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

4.1Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the *school* Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
  - Setting appropriate privacy levels on their personal accounts/sites.
  - Being aware of the implications of using location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Using strong passwords.
  - Ensuring staff do not represent their personal views as being that of the *school.*

- Members of staff are encouraged not to identify themselves as employees of Rodmersham School on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.
- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues, will not be shared or discussed on social media sites.
- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

4.2 Communicating with learners and their families

- Staff will not use any personal social media accounts to contact learners or their family members.
- All members of staff are advised not to communicate with or add any current or past learners or their family members, as 'friends' on any personal social media accounts.
- Any communication from learners and parents/carers received on personal social media accounts will be reported to the DSL (or deputy)/ the *headteacher..*
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the *headteacher.* Decisions made and advice provided in these situations will be formally recorded to safeguard learners, members of staff and the setting.
- If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

5. Official use of social media

- Rodmersham School works with official social media channel, Twitter.
- The official use of social media sites by Rodmersham School only takes place with clear educational or community engagement objectives and with specific intended outcomes and the use has been formally risk assessed and approved by the *headteacher* prior to use.
- Official social media sites are suitably protected and, where possible, run linked our website.
  - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage official social media channels.
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.

- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with learners; any official social media activity involving learners will be moderated if possible and written parental consent will be obtained as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Read and understand our Acceptable Use Policy.
  - Be aware they are an ambassador for the *school*.
  - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
  - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any private or direct messaging with current or past learners or their family members.
  - Inform their line manager, the DSL (or deputy) and/or the *headteacher* of any concerns, such as criticism, inappropriate content or contact from learners.

6. Learners' use of social media

- The use of social media during *school* hours for personal use *is not* permitted for learners.
- Rodmersham School will empower our learners to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive safeguarding education

approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies, including our PSHE Policy.

- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for learners under the required age as outlined in the services terms and conditions.
- Learners will be advised:
    - to consider the benefits and risks of sharing personal details or information on social media sites which could identify them and/or their location.
    - to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.
    - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
    - to use safe passwords.
    - to use social media sites which are appropriate for their age and abilities.
    - how to block and report unwanted communications.
    - how to report concerns on social media, both within the setting and externally.

- Any concerns regarding learners use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.
- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.
- Sanctions and/or pastoral/welfare support will be implemented and offered to learners as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.
- Concerns regarding learners use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

7. Policy monitoring and review

- Technology evolves and changes rapidly. Rodmersham School will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.
- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

8. Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing *school* policies and procedures. This includes: ***The Staff Code of Conduct Policy and The Child Protection Policy.***
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and learners to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or *headteacher* will seek advice from the Education People's Education Safeguarding Service or other agency in accordance with our child protection policy.

Part Four
Acceptable Use of Technology

Early Years and Key Stage 1 (0-6)

I understand that the school Acceptable Use Policy will help keep me safe and happy online.

- I only use the internet when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information and passwords safe.
- I only send messages online which are polite and friendly.
- I know the school can see what I am doing online when I use school computers and tablets, including when I am at home.
- I always tell an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that if I do not follow the rules:
    - ***Mrs McMullon will contact my parents/guardians***
    - ***I will not be able to use technology without supervision.***
- I have read and talked about these rules with my parents/carers

Shortened KS1 version (e.g. for use on posters)

- I only go online with a grown-up.
- I am kind online.
- I keep information about me safe online.
- I tell a grown-up if something online makes me unhappy or worried.

Key Stage 2 (7-11)

I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.

Safe

- I will behave online the same way as I behave in the classroom.
- I only send messages which are polite and friendly.
- I will only post pictures or videos on the internet if they are safe and appropriate, and if I have permission.
- I only talk with, and open messages, from people I know.
- I will only click on links if I know they are safe.

- I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult.

Learning

- I always ask permission from an adult before using the internet.
- I only use websites and search engines that my teacher has chosen.
- I use school devices for school work unless I have permission otherwise.
- If I need to learn online at home, I will follow the school remote learning AUP.

Trust

- I know that not everything or everyone online is honest or truthful.
- I will check content on various sources like other websites, books or with a trusted adult.
- I always credit the person or source that created any work, images, or text I use.

Responsible

- I keep my personal information safe and private online.
- I will keep my passwords safe and will not share them.
- I will not access or change other people's files or information.
- I will only change the settings on a device if a member of staff has allowed me to.

Understand

- I understand that the school internet filter is there to protect me, and I will not try to bypass it.
- I know that all school devices and systems are monitored to help keep me safe, including when I use them at home.
- I have read and talked about these rules with my parents/carers.
- I can visit www.thinkuknow.co.uk and www.childline.org.uk to learn more about being safe online.
- I know that if I do not follow the school rules then:
  - ***Mrs Mullon will contact my parents/guardians***
  - ***I will have to be supervised when using technology for learning***

Tell

- If I see anything online that I should not or that makes me feel worried or upset, I will minimise the page and tell an adult straight away.
- If I am aware of anyone being unsafe with technology, I will report it to a teacher.
- I know it is not my fault if I see, or someone sends me, something bad online. I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened.

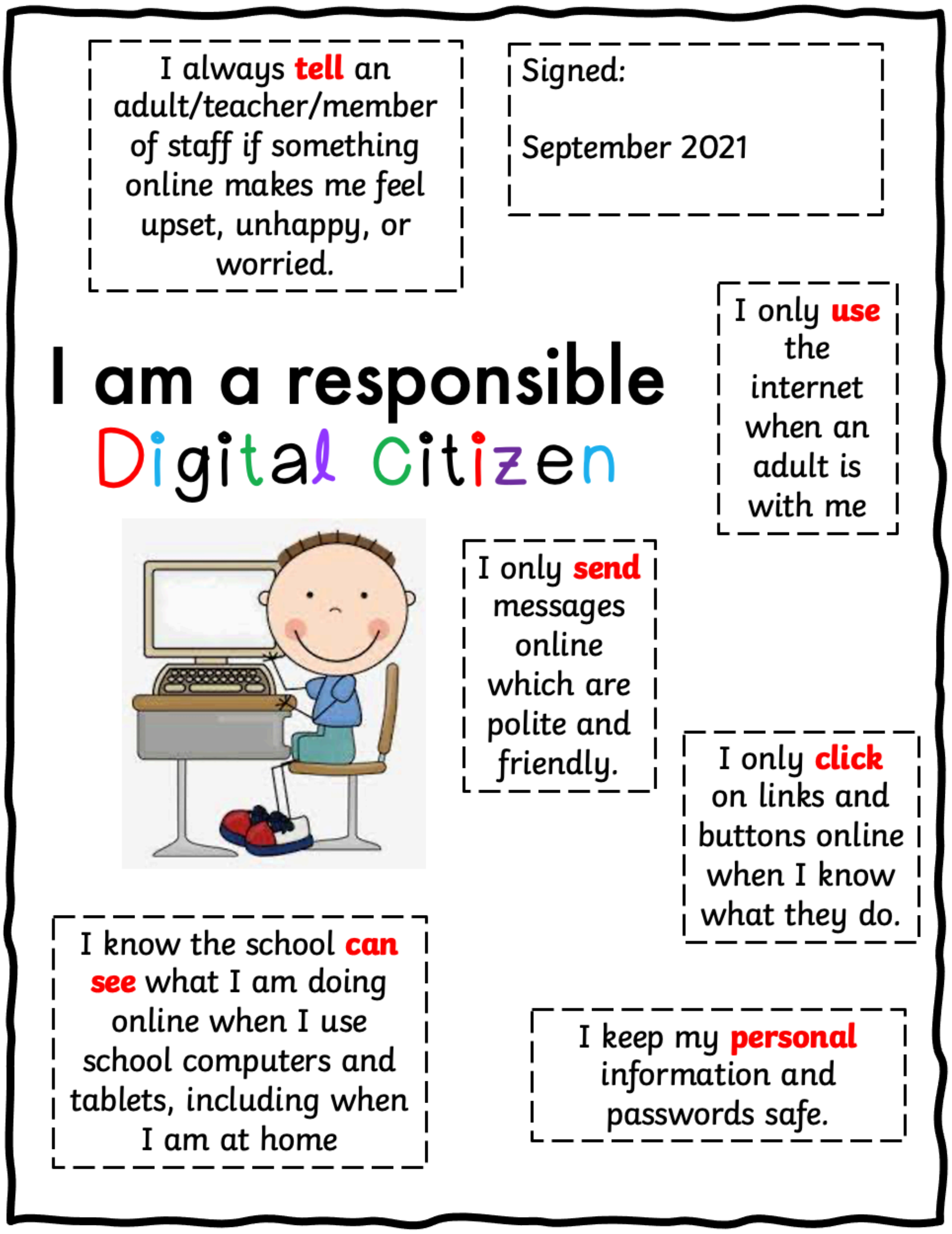
Alternative KS2 Statements *(With thanks to Kingsnorth Primary School)*

- I understand that the school Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in school for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my school name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school.
- If, for any reason, I need to bring a personal/smart device and/or mobile phone into school I know that it is to be handed in to the office and then collected at the end of the school day.
- I know that all school devices/computers and systems are monitored, including when I am using them at home.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Shortened KS2 version (for use on posters)

- I ask a teacher about which websites I can use.
- I will not assume information online is true.
- I know there are laws that stop me copying online content.

- I know I must only open online messages that are safe. If I am unsure, I will not open it without speaking to an adult first.
- I know that people online are strangers, and they may not always be who they say they are.
- If someone online suggests meeting up, I will always talk to an adult straight away.
- I will not use technology to be unkind to people.
- I will keep information about me and my passwords private.
- I always talk to an adult if I see something which makes me feel worried.



I always **tell** an adult/teacher/member of staff if something online makes me feel upset, unhappy, or worried.

Signed:

September 2021

I am a responsible Digital Citizen

I only **use** the internet when an adult is with me

I only **send** messages online which are polite and friendly.

I only **click** on links and buttons online when I know what they do.

I know the school **can see** what I am doing online when I use school computers and tablets, including when I am at home

I keep my **personal** information and passwords safe.

Acceptable Use of Technology Statements and Forms for Parents/Guardians

Parent/Carer AUP Acknowledgement

Rodmersham School Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Rodmersham School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.

2. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

3. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

4. I am aware that the school policy states that my child cannot use personal device and mobile/smart technology on site and that should my child need to bring a mobile device to school then it will be handed into the office to ensure it is kept safe ans secure. It will be handed back at the end of the day.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

6. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

7. I and my child, are aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

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

9. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the schoolcommunity's safety online.

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

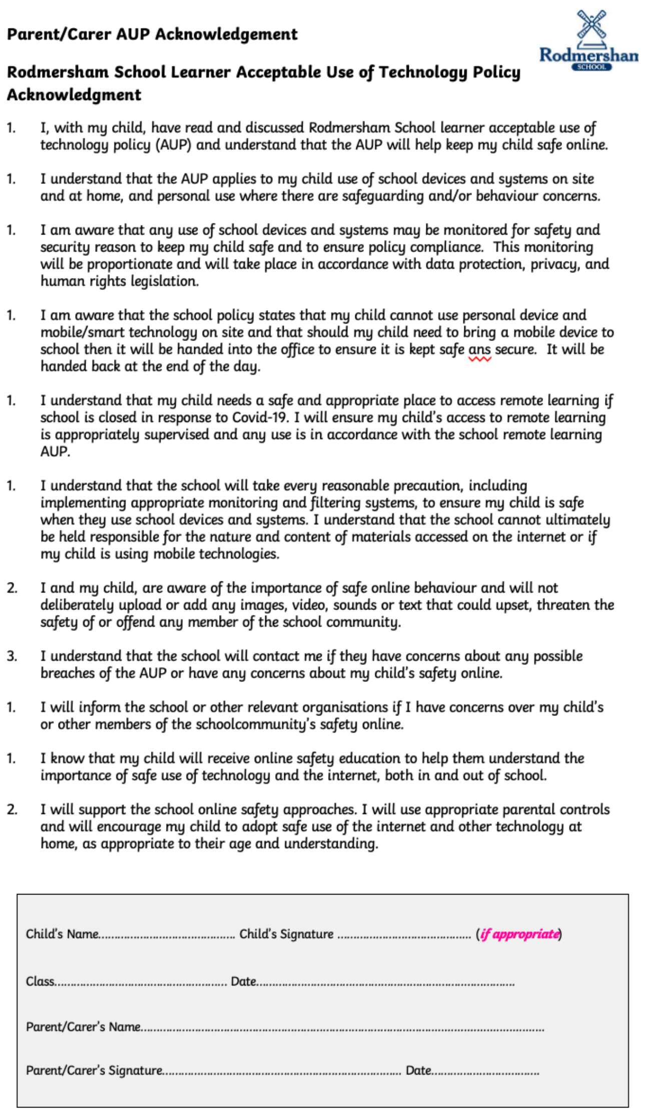
11. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name... Child's Signature .... (***if appropriate***)

Class.. Date...

Parent/Carer's Name...

Parent/Carer's Signature.. Date................................



Parent/Carer AUP Acknowledgement

Rodmersham School Learner Acceptable Use of Technology Policy Acknowledgment

1. I, with my child, have read and discussed Rodmersham School learner acceptable use of technology policy (AUP) and understand that the AUP will help keep my child safe online.

1. I understand that the AUP applies to my child use of school devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns.

1. I am aware that any use of school devices and systems may be monitored for safety and security reason to keep my child safe and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

1. I am aware that the school policy states that my child cannot use personal device and mobile/smart technology on site and that should my child need to bring a mobile device to school then it will be handed into the office to ensure it is kept safe ans secure. It will be handed back at the end of the day.

1. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

1. I understand that the school will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school devices and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using mobile technologies.

2. I and my child, are aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

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

1. I will inform the school or other relevant organisations if I have concerns over my child's or other members of the schoolcommunity's safety online.

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

2. I will support the school online safety approaches. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

Child's Name... Child's Signature .... (***if appropriate***)

Class.. Date...

Parent/Carer's Name...

Parent/Carer's Signature.. Date................................

Parent/Carer Acceptable Use of Technology Policy

1. I know that my child will be provided with internet access and will use a range of IT systems, in order to access the curriculum and be prepared for modern life whilst at Rodmersham School

2. I am aware that learners use of mobile technology and devices, such as mobile phones, is not permitted at Rodmersham.

3. I am aware that any internet and technology use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the school systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.

4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the school internet and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

5. I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school remote learning AUP.

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

7. I have read and discussed Rodmersham School learner Acceptable Use of Technology Policy (AUP) with my child.

8. I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.

9. I know I can seek support from the school about online safety, such as via the school website (https://www.rodmersham.kent.sch.uk), to help keep my child safe online at home.

10. I will support the school approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.

11. I, together with my child, will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

12. I understand that a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.

13. I understand that if I or my child do not abide by the Rodmersham School AUP, appropriate action will be taken. This could include sanctions being applied in line with the school policies and if a criminal offence has been committed, the police being contacted.

14. I know that I can speak to the Designated Safeguarding Lead (Nicky McMullon), or my child's class teacher if I have any concerns about online safety.

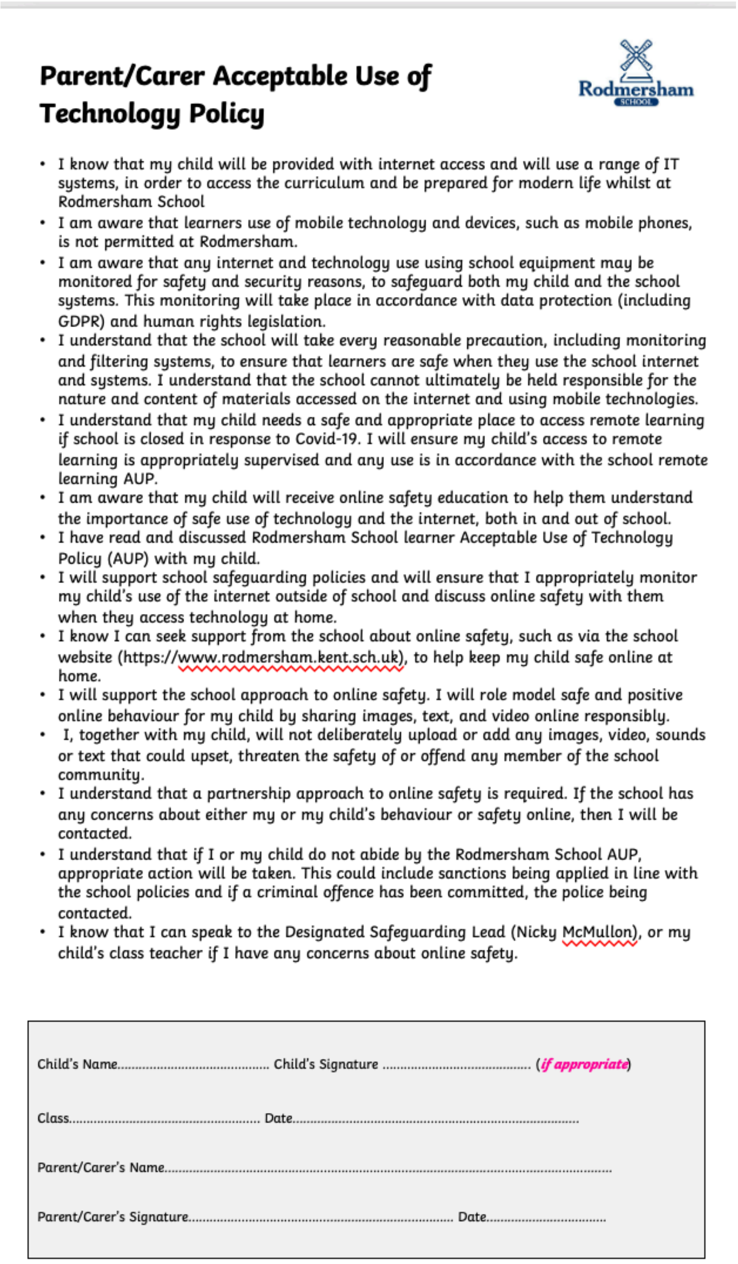
I have read, understood and agree to comply with the Rodmersham School Parent/Carer Acceptable Use of Technology Policy.

Child's Name... Child's Signature .... (*if appropriate*)

Class.. Date..

Parent/Carer's Name..

Parent/Carer's Signature.. Date................................



Parent/Carer Acceptable Use of Technology Policy

- I know that my child will be provided with internet access and will use a range of IT systems, in order to access the curriculum and be prepared for modern life whilst at Rodmersham School
- I am aware that learners use of mobile technology and devices, such as mobile phones, is not permitted at Rodmersham.
- I am aware that any internet and technology use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the school systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that learners are safe when they use the school internet and systems. I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my child needs a safe and appropriate place to access remote learning if school is closed in response to Covid-19. I will ensure my child's access to remote learning is appropriately supervised and any use is in accordance with the school remote learning AUP.
- I am aware that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I have read and discussed Rodmersham School learner Acceptable Use of Technology Policy (AUP) with my child.
- I will support school safeguarding policies and will ensure that I appropriately monitor my child's use of the internet outside of school and discuss online safety with them when they access technology at home.
- I know I can seek support from the school about online safety, such as via the school website (https://www.rodmersham.kent.sch.uk), to help keep my child safe online at home.
- I will support the school approach to online safety. I will role model safe and positive online behaviour for my child by sharing images, text, and video online responsibly.
- I, together with my child, will not deliberately 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 a partnership approach to online safety is required. If the school has any concerns about either my or my child's behaviour or safety online, then I will be contacted.
- I understand that if I or my child do not abide by the Rodmersham School AUP, appropriate action will be taken. This could include sanctions being applied in line with the school policies and if a criminal offence has been committed, the police being contacted.
- I know that I can speak to the Designated Safeguarding Lead (Nicky McMullon), or my child's class teacher if I have any concerns about online safety.

Child's Name... Child's Signature .... (*if appropriate*)

Class.. Date..

Parent/Carer's Name..

Parent/Carer's Signature.. Date................................

Acceptable Use of Technology for Staff, Visitors and Volunteers

Staff Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Rodmersham School 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 Rodmersham School 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.

Policy Scope

1. 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 Rodmersham School both professionally and personally. 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**.**

2. I understand that Rodmersham School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school staff code of conduct and remote learning AUP.

3. 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.

Use of School Devices and Systems

4. 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.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed at the Had teachers description, depending on the intended outcome.

6. Where I deliver or support remote learning, I will comply with the school remote learning AUP.

Data and System Security

7. 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.
    - I will protect the devices in my care from unapproved access or theft, by not leaving them unsupervised.
    -

8. I will respect school system security and will not disclose my password or security information to others.

9. 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 head teacher.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the head teacher.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school information security policies..

    - 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.

12. 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 provided VPN.

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

14. 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.

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

16. 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 Support Provider (Dave Boulden) as soon as possible.

17. If I have lost any school related documents or files, I will report this to the ICT Support Provider (Dave Boulden) school Data Protection Officer (Alison Presdee Colley) as soon as possible.

18. Any images or videos of learners will only be used as stated with the relevant permissions. I understand images of learners must always be appropriate and should only be taken with school provided equipment and only be taken/published where learners and/or parent/carers have given explicit written consent.

Classroom Practice

19. I am aware of the expectations relating to safe technology use in the classroom and safe remote learning.

20. I have read and understood the school mobile technology and social media policies..

21. I will promote online safety with the learners in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where learners feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) (Nicky McMullon) or a deputy (Maria Cooper or Justine Williams) as part of planning online safety lessons or activities to ensure support is in place for any learners who may be impacted by the content.
    - make informed decisions to ensure any online safety resources used with learners is appropriate.

22. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school child protection policies.

23. 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.

Mobile Devices and Smart Technology

24. 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 code of conduct and the school mobile technology policy and the law.

Online Communication, including Use of Social Media

25. 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 staff code of conduct, the school social media policy and the law. In line with the school social media policy:

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

26. My electronic communications with current and past learners and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

    - I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school email address, user account or telephone number.
    - I will not share any personal contact information or details with learners, such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past learners and/or their parents/carers.
    - If I am approached online by a current or past learner or parents/carer, I will not respond and will report the communication to my Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP will be discussed with the DSL and/or headteacher.

Policy Concerns

27. 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.

28. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

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

30. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the DSL in line with the schoolchild protection policy.

31. I will report concerns about the welfare, safety, or behaviour of staff to the headteache in line with the allegations against staff polic

Policy Compliance and Breaches

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

33. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

34. I understand that if the school believe that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff code of conduct.

35. I understand that if the school believe 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 code of conduct.

36. 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 Rodmersham School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ....

Signed: ....

Date (DDMMYY)..

Visitor and Volunteer Acceptable Use of Technology Policy

As a professional organisation with responsibility for safeguarding, it is important that all members of the community, including visitors and volunteers, are aware of our behaviour expectations and their professional responsibilities when using technology.

This AUP will help Rodmersham School ensure that all visitors and volunteers understand the schools expectations regarding safe and responsible technology use.

Policy Scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services provided to me or accessed as part of my role within Rodmersham School both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning systems and communication technologies.

2. I understand that Rodmersham School AUP should be read and followed in line with the school staff code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; visitors and volunteers should ensure that all 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.

Data and Image Use

4. I will ensure that any access to personal data is kept in accordance with Data Protection legislation, including GDPR.

5. I understand that I am allowed to take images or videos of learners but only with permission from the Head Teacher who has sought permission from the appropriate parent/guardian.

Classroom Practice

6. I am aware of the expectations regarding safe use of technology in the classroom and other working spaces, including appropriate supervision of learners.

7. Where I deliver or support remote learning, I will comply with the school remote learning AUP.

8. I will support staff in reinforcing safe behaviour whenever technology is used on site and I will promote online safety with the children in my care.

9. I will immediately report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the Designated Safeguarding Lead (DSL) (Nicky McMullon) in line with the school's child protection policy.

10. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music is protected, I will not copy, share, or distribute or use it.

Use of Mobile Devices and Smart Technology

11. In line with the school mobile technology policy, I understand that....
Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

- They understand that any activity on a school device or using school networks/platforms/internet may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
- They will leave their phone in their pocket and turned off. Under no circumstances will they use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), they will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
- If they are given access to school-owned devices, networks, cloud platforms or other technology:
    - They will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - They will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of their role
    - They will not attempt to make contact with any pupils/students or to gain any contact details under any circumstances
    - They will protect their user name/password and notify the school of any concerns
    - They will abide by the terms of the school Data Protection Policy
- They will not share any information about the school or members of its community that they gain as a result of their visit in any way or on any platform except where relevant to the purpose of their visit and agreed in advance with the school.
- They will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
- They will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils/students and will not give any advice on online-safety issues unless this is the purpose of their visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).

- They will only use any technology during their visit, whether provided by the school or their personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to their visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

Online Communication, including the Use of Social Media

12. I will ensure that my online reputation and use of technology and is compatible with my role within the school. This includes my use of email, text, social media, social networking, gaming and any other personal devices or websites.
    - I will take appropriate steps to protect myself online as outlined in the online safety/social media policy ..
    - I will not discuss or share data or information relating to learners, staff, school business or parents/carers on social media.
    - I will ensure that my use of technology and the internet will not undermine my role, interfere with my duties and will be in accordance with the staff code of conduct and the law.

13. My electronic communications with learners, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.
    - All communication will take place via school approved communication channels such as via a school provided email address, account or telephone number.
    - Communication will not take place via personal devices or communication channels such as via my personal email, social networking account or mobile phone number.
    - Any pre-existing relationships or situations that may compromise this will be discussed with the DSL (Nicky McMullon).

Policy Compliance, Breaches or Concerns

14. 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 Designated Safeguarding Lead (Nicky McMullon).

15. 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.

16. I will not attempt to access, create, transmit, display, publish or forward any material or content online that is inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

17. 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.

18. I understand that the school may exercise its right to monitor the use of school information systems, including internet access and the interception of emails, to monitor policy compliance and to ensure the safety of learners, staff and visitors/volunteers. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

19. I will report and record concerns about the welfare, safety or behaviour of learners or parents/carers to the Designated Safeguarding Lead (Nicky McMullon) in line with the school child protection policy.

20. I will report concerns about the welfare, safety, or behaviour of staff to the headteacher, in line with the allegations against staff policy.

21. I understand that if the school believes that unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour is taking place online, the school may invoke its disciplinary procedures.

22. 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 Rodmersham School visitor/volunteer Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of visitor/volunteer: ....

Signed: ....

Date (DDMMYY)..

Wi-Fi Acceptable Use Policy

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

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

1. The school provides Wi-Fi for the school community and allows access for educational purposes only.

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

3. The use of technology falls under Rodmersham School Acceptable Use of Technology Policy (AUP), online safety policy and anti bullying policy which all learners/staff/visitors and volunteers must agree to and comply with.

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

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

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

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

8. The school accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity

theft, spyware, plug-ins or other internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

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

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

11. My use of school WI-Fi will be safe and responsible and will always be in accordance with the school AUP and the law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

12. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

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

14. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead (Nicky McMullon).

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

I have read, understood and agreed to comply with Rodmersham School Wi-Fi acceptable Use Policy.

Name ....

Signed: ....Date (DDMMYY)........................

Acceptable Use Policy (AUP) for Remote Learning

This content can either be used to create a standalone AUP or can be integrated into existing documents according to setting preference.

These templates specifically address safer practice when running formal remote learning, including live streamed sessions, but can also apply to other online communication, such as remote parent meetings or pastoral activities. Settings should implement the approaches that best suit the needs of their community following appropriate discussions.

A remote learning AUP should be implemented following a thorough evaluation of remote learning tools with approval from leadership staff. We recommend settings use existing systems and/or education focused platforms where possible, and that staff only use approved accounts and services to communicate with learners and/or parents/carers.

Additional information and guides on specific platforms can be found at:

- https://coronavirus.lgfl.net/safeguarding
- https://swgfl.org.uk/resources/safe-remote-learning/video-conferencing-for-kids-safeguarding-and-privacy-overview/

Further information and guidance for SLT and DSLs regarding remote learning:

- Local guidance:
    - Kelsi:
        - Guidance for Full Opening in September
        - Online Safety Guidance for the Full Opening of Schools
    - The Education People: Covid-19 Specific Safeguarding Guidance and Resources
        - 'Safer remote learning during Covid-19: Information for School Leaders and DSLs'
- National guidance:
    - DfE:
        - 'Safeguarding and remote education during coronavirus (COVID-19)
    - SWGfL:
        - Safer Remote Learning
    - LGfL: Coronavirus Safeguarding Guidance
    - NSPCC:
        - Undertaking remote teaching safely
    - Safer Recruitment Consortium:
        - 'Guidance for safer working practice for those working with children and young people in education settings Addendum' April 2020

Remote Learning AUP Template - Staff Statements

Rodmersham School Staff Remote Learning AUP

The Remote Learning Acceptable Use Policy (AUP) is in place to safeguarding all members of school **name** community when taking part in remote learning following any full or partial **school** closures.

Leadership Oversight and Approval

1. Remote learning will only take place using **Microsoft Teams.**
    - **Microsoft Teams** has been assessed and approved by **the headteacher/a member of Senior Leadership Team (SLT)**.
2. Staff will only use **school** managed **or** specific, approved professional accounts with learners **and/or** parents/carers.
    - Use of any personal accounts to communicate with learners and/or parents/carers is not permitted.
        - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with **Nicky McMullon,** Designated Safeguarding Lead (DSL).
    - Staff will use work provided equipment where possible **e.g. a school laptop, tablet, or other mobile device.**
3. Online contact with learners **and/or** parents/carers will not take place outside of the operating times as defined by SLT:
    - **8:40 – 3:30**
4. All remote lessons will be formally timetabled; **a member of SLT, DSL and/or head of department** is able to drop in at any time.
5. Live-streamed remote learning sessions will only be held with approval and agreement from **the headteacher/a member of SLT.**

Data Protection and Security

6. Any personal data used by staff and captured by **Microsoft Teams** when delivering remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.
7. All remote learning and any other online communication will take place in line with current **school** confidentiality expectations as outlined in **the Staff Code of Conduct**.
8. All participants will be made aware that **Microsoft Teams** records activity when activated. Permission will be sought by the appropriate guardian/parent.
9. Staff will not record lessons or meetings using personal equipment unless agreed and risk assessed by SLT and in line with our data protection policy requirements.
10. Only members of the Rodmersham School community will be given access to **Microsoft Teams**.
11. Access to **Microsoft Teams** will be managed in line with current IT security expectations as outlined in **this policy**.

Session Management

12. Staff will record the length, time, date, and attendance of any sessions held.

13. Appropriate privacy and safety settings will be used to manage access and interactions. This includes but is not exhausted too:
   - Using breakout rooms
   - Using waiting rooms
   - Chat disabled
   - No screen sharing between learners

   - contact will be made via learners' **school** provided email accounts.
   - contact will be made via a parents/carer's account.
   - staff will **mute/disable** learners' videos and microphones.
   - at least 1 member of staff will be present.
     - If this is not possible, SLT approval will be sought.

14. Live 1:1 sessions will only take place with approval from the **headteacher**.
15. A pre-agreed **invitation** detailing the session expectations will be sent to those invited to attend.
    - Access links should not be made public or shared by participants.
    - Learners **and/or** parents/carers should not forward or share access links.
    - If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
    - Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
16. Alternative approaches **or** access will be provided to those who do not have access.

Behaviour Expectations

17. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom.
18. All participants are expected to behave in line with existing **school** policies and expectations. This includes:
    - **Appropriate language will be used by all attendees.**
    - **Staff will not take or record images for their own personal use.**
    - **Setting decisions about if other attendees can or cannot record events for their own use, and if so, any expectations or restrictions about onward sharing.**
19. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.
20. When sharing videos and/or live streaming, participants are required to:
    - ***wear appropriate dress.***
    - ***ensure backgrounds of videos are neutral (blurred if possible).***
    - ***ensure that personal information and/or unsuitable personal items are not visible, either on screen or in video backgrounds.***
21. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

Policy Breaches and Reporting Concerns

22. Participants are encouraged to report concerns during remote live-streamed sessions:
    - **To a member of staff**
    - **To the headteacher**
    - **To a member of staff on private chat.**
23. If inappropriate language or behaviour takes place, participants involved will be removed by staff, the session may be terminated, and concerns will be reported to **Nicky McMullon, Head Teacher**.
24. Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying and behaviour.
25. Sanctions for deliberate misuse may include:**. restricting/removing use, contacting police if a criminal offence has been committed, speaking with parents to resolve the issue.**
26. Any safeguarding concerns will be reported to **Nicky McMullon**, Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Rodmersham School Acceptable Use Policy (AUP) for remote learning.

Staff Member Name: ....

Date..