TWO RIVERS
HIGH SCHOOL

ONLINE SAFETY POLICY

Two Rivers School

LR SPR 23 / NR SPR 24

Last Review Date:		Spring Term 2023
Next Review Date:		Spring Term 2024
Committee:		Curriculum & Learning Committee
Review Cycle:		1 YEAR
Statutory Policy:		Yes
Date	**Version**	**Reason for change**
07.03.2023	V1.0	New Policy Drafting

This policy is available on our school websites and is available on request from the School Office. We also inform parents and carers about this policy when their children join our schools and through our school newsletters.

Index Page

This policy will be reviewed at regular intervals to reflect changes regarding advice within education policy and following analysis of online behaviour trends at Two Rivers School. The policy and guidance will be reviewed by the Senior Leadership Team and the Local Governing Committee.

This Online Safety Policy outlines the commitment of Two Rivers School to safeguard members of our school community online in accordance with statutory guidance and best practice. The policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of our school digital systems, both in and out of the school sites. It also applies to the use of personal digital technology on the school sites (where allowed).

Should serious online safety incidents occur, the relevant external persons/agencies will be informed, such as the LA Safeguarding Officer, LADO, or the police.

1. Aims

Two Rivers School is dedicated to all students being able to contribute fully and positively to their wider community. This policy is in place with the following aims:

- To ensure all who work and study at Two Rivers School are safeguarded from potentially harmful and inappropriate online material.
- To help limit the risks of working online, such as
  - Access to inappropriate or harmful content
  - The access to or sharing of personal information
  - Cyber-bullying
  - Grooming
  - The potential to over reliance on online communication
- To identify the risks to which people could be exposed, along with the steps that the school will take to avoid them.
- To clarify how we protect and educate our students and staff, in their use of technology and establish mechanisms for us to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk, as stated in Keeping Children Safe in Education 2023 .:

- **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 (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

2. Ethos

At Two Rivers School, the children's welfare is of paramount importance to us, and we are a child centred school. Our children are reassured that they have a voice, will be listened to, and what they say will be taken seriously.

3. Legislation, guidance and links to other policies

As part of the statutory duty for Two Rivers School to promote students' wellbeing, schools have a clear role to play in the management of students' behaviour. To support this, the Government's Education and Inspections Act 2006, ensures that school staff have the information, advice and power to:

- Discipline students whose behaviour is unacceptable, who break the school rules or who fail to follow a reasonable instruction (Section 90 and 91 of the Education and Inspections Act 2006).
- The power also applies to all paid staff (unless the Executive Headteacher/Headteacher says otherwise) with responsibility for students, such as teaching assistants.
- Discipline students at any time the student is in school or elsewhere under the charge of a teacher, including on school visits.
- Discipline students in certain circumstances when a student's misbehaviour occurs outside of school.
- Confiscate students' property.

The school understands it has a safeguarding duty, in respect of all of its students, regarding appropriate online behaviour as per the Keeping Children Safe in Education 2023 statutory guidance. The school will share relevant data to the Local Authority and other relevant professionals as required. Please read this policy alongside the school's Behaviour Management, Health and Safety, Supporting Pupils with Medical Conditions, and Safeguarding policies.

Two Rivers School will also follow anti-discrimination law. All staff will act to prevent discrimination, harassment, and victimisation within the school, including if this takes place online. This applies to all schools in England and Wales, and most schools in Scotland.

This policy should also be read alongside the following policies which can be found on our website www.tworiversschool.net:

- Antibullying Policy
- Attendance Policy
- Behaviour Policy
- Positive Management of Severe Challenging Behaviour Policy
- Child on Child Abuse Policy
- Safeguarding Policy

4. Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

The Local Governing Board:
Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Online Safety Link Governor, to include:

- regular meetings with the Online Safety Co-Ordinator
- receiving regular summaries of online safety incidents
- receiving regular updates detailing changes made to the filtering systems
- reporting to relevant governors' meetings

- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

The Local Governing Board will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Executive Headteacher/Headteacher and Senior Leaders:

- The Executive Headteacher/Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, through the day-to-day responsibility for online safety which may be delegated to the Online Safety Lead.
- The Executive Headteacher/Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Executive Headteacher/Headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Executive Headteacher/Headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Executive Headteacher/Headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead:

At Two Rivers High School this is the Designated Safeguarding Lead and the Computing Lead and Deputy Headteacher at Two Rivers Primary School.

The DfE guidance "Keeping Children Safe in Education" (2023) states:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."*

The role includes:

- take day to day responsibility for online safety issues, being aware of the potential of serious child protection concerns
- has a leading role in establishing and reviewing the school online safety policies
- promotes an awareness of and commitment to online safety education and awareness raising across the school and beyond
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- liaises with relevant curriculum staff to ensure that online safety curriculum is planned, mapped, embedded, and evaluated
- provides training and advice for staff

- liaises with the Local Authority and relevant agencies
- liaises with school technical staff
- signs off changes to the filtering/monitoring systems
- receives reports of online safety incidents and uses these to inform future online safety developments
- meets regularly with the Online Safety Nominated Link Governor to discuss current issues, review incident logs and filtering
- attends relevant Local Governing Committee meetings
- reports regularly to the Senior Leadership Team

Designated Safeguarding Lead (DSL):
The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate online contact with adults/strangers
- potential or actual incidents of grooming
- online bullying

Network Manager/IT Manager:
The Network Manager is responsible for ensuring:

- they are aware of this policy and the ICT Security Policy so they can carry out their work effectively and in line with policy
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Academy Group Online Safety Guidance that may apply.
- that users may only access the networks and devices through a password, as detailed in the school's ICT Security Policy
- filtering is documented within the ICT Security Policy, which is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network, internet, Learning Platform, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Executive Headteacher/Headteacher and/or Online Safety Lead for investigation, action, and sanction, as necessary
- that monitoring software and systems are implemented and updated as agreed in MAT/school policies.

Curriculum Leads:
Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:

- IT lessons
- PHSE and SRE programmes
- A mapped cross-curricular programme
- Assemblies and pastoral programmes

- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support staff:

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff Acceptable Use Agreement (AUA)
- they immediately report any suspected misuse or problem to the Online Safety Lead for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all relevant aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and Acceptable Use Agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Students:

- are responsible for using the school digital technology systems in accordance with the Learner Acceptable Use Agreement and Online Safety Policy, which includes handing in their mobile phones should they bring them onto the school site
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through Parents' Evenings, newsletters, letters, website and information about national / local online safety campaigns. Parents and carers can also access National Online Safety to gain up to date information regarding online safety to enable them to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of technology.

5. Online Safety Committee

The Committee includes:

- the Online Safety Lead
- Executive Headteacher (Primary School)
- the ICT teachers (High School)
- PSHE Lead
- a nominated Governor
- IT Manager/Technician

The group's responsibility is to:

- Review the Online Safety Policy
- Review school filtering systems and procedures and request changes if needed
- map and review the online safety education provision – ensuring relevance, breadth and progression and coverage
- analyse and take relevant action based upon incident logs

6. Education

Online safety is an important focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. It is important that our students learn to take responsibility to enable them to be successful and be independent. The Online Safety Curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety Curriculum for all year groups, taught within appropriate areas such as IT, Computing, SMSC, RHSE/RSE. These are reviewed regularly.
- Key online safety messages are reinforced as required via assemblies or through relevant national initiatives and opportunities e.g. Being Safe and Healthy week, Safer Internet Day and Anti-bullying week
- Lessons are matched to need; are age-related and adapted to meet the individual needs of our learners, but will build on prior learning
- Students will be taught how to be critical of the information they find online.
- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- learners should be helped to understand the need for the Learner Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- staff should act as good role models in their use of digital technologies the internet and mobile devices.

7. Network Safety

The school's network is managed by the in-house support team. The team is responsible for the safety of the network and the students, staff and community users who access it.

Filtering

- RM Firewall safeguards that only appropriate content is viewed by users.
- the school's filtering is documented in the ICT Security Policy and is agreed by the Online Safety Committee. These are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents or behaviours
- the school manages access to content across its systems for all users.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- routes for reporting inappropriate content include the use of Smoothwall Monitor, contacting IT support, and the use of MyConcern. This provides a clear process to deal with requests for filtering changes

Monitoring

- The school monitors all network use across all its devices and services.
- Smoothwall is used to monitor all users, and users are aware that the network is monitored. Reports regarding student breaches are sent to the DSL and DDSL (High School) and the Computing Lead (Primary School), and staff breaches are sent to the DSL and Deputy Headteacher (High School) and the Executive Headteacher (Primary School). Any reports of abuse or misuse are acted upon within an efficient time frame, with rapid safeguarding intervention taken if required.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

Technical Safety

- There will be regular reviews and audits of the safety and security of the school technical systems by the IT Manager/Technician
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the school's technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password and should never share these with anyone else.

8. Mobile Technologies:

Mobile technology devices may be school owned or personally owned. These could include: a smartphone, tablet, notebook / laptop or other technology, that usually has the capability of using the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, students and parents/carers will give consideration to the use of mobile technologies. No one should use a mobile phone on site, apart from an adult who may use it when in designated spaces e.g. the staffroom, off-site, SLT offices, where there isn't a presence of children. There are exceptional circumstances these are at the discretion of the Executive Headteacher, Headteacher or Deputy Headteacher.

Please see **Appendix A, B and C** for a copy of the Acceptable Use Agreements.

9. Social Media

The school understands that it has a duty to protect its learners, the school, and the individual when publishing any material online. All staff and adults working with children are in a position of trust and their conduct needs to reflect this. The school will provide a safe learning environment for the learners and staff.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media
- do not post images from inside the school building using personal social media
- they do not converse with students, parents and carers using direct messages through social media, and report all attempts of contact from parents, carers and students to SLT (reference to Low Level Concern Policy).

When official school social media accounts are established, there will be:

- approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff (IT Manager and Deputy Headteacher at High School and Secretary and Assistant Headteacher at Primary School)
- a code of behaviour for users of the accounts
- systems for dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer.
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours within break time.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

- The school reserves the right to legitimately and proportionately monitor employees' internet, email and social media usage on school computers and mobile devices. The monitoring may include but it not limited to monitoring, accessing, reviewing, and printing or any social media material. This information may be disclosed to a third party.

The contents of the school's IT and communication system are the property of the organisation. Colleagues should have no expectations of privacy in any social media post or message transmitted from or to, received, stored, or recorded on the organisation's IT and communications systems. Therefore, colleagues are advised not to use the organisation's IT equipment for any personal matter they wish to keep private or confidential from their employer.

Disciplinary action over Social Media use

All employees are required to adhere to this policy. Employees should note that any breaches of this policy may lead to disciplinary action, including dismissal. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing serious damage to the organisation, may constitute gross misconduct and lead to summary dismissal.

An employee who makes a defamatory statement that is published on the internet or who harasses an individual, may be legally liable for any damage to the reputation of the individual or organisation concerned.

Data Protection

The organisation will comply with the provisions of Data Protection law. Personal data will be processed by the organisation in accordance with the principles of that legislation, as necessary for the performance of the employee's contract of employment and/or the conduct of the organisation's business. The organisation will ensure that personal information about an employee is securely retained in line with GDPR.

Links with other policies:

- Grievance Policy
- Disciplinary Policy
- ICT Security Policy
- Safeguarding
- Equal Opportunities / Bullying and Harassment Policy
- Data Protection Policy

10. Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with the Online Safety Policy
- learners' full names will not be used anywhere on a website or Facebook, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school Data Protection Policy
- images will be securely stored in line with the school Retention Policy

11. Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed by the IT Manager and Deputy Headteacher at High School and the Executive Headteacher and Secretary at Primary School. The website is hosted by (BUe4Education). The school ensures that the Online Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

12. Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents
If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, these will be reported to the police. Such incidents may include, but not be limited to:

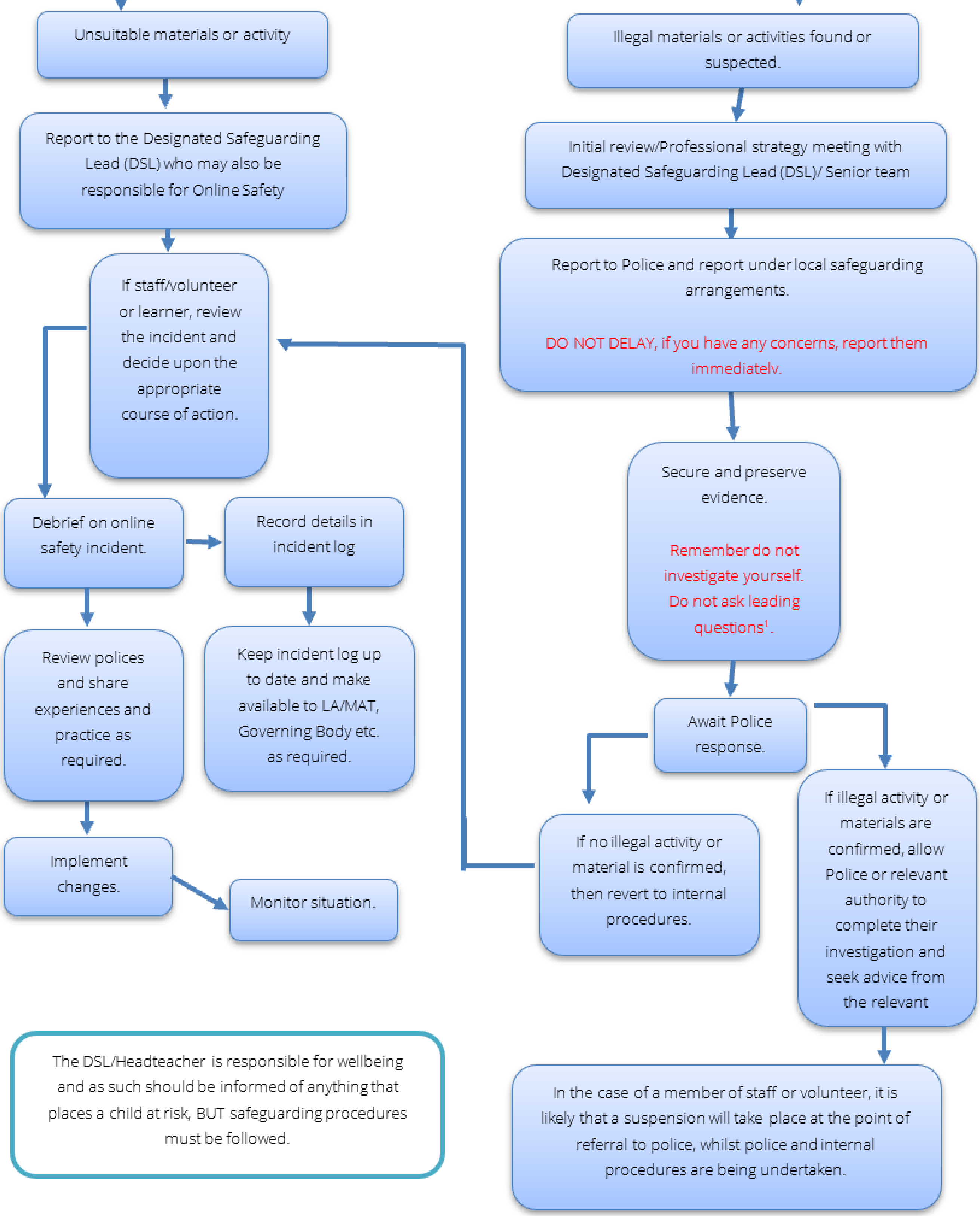
- Child sexual abuse imagery
- Child sexual abuse/exploitation/grooming
- Terrorism
- Encouraging or assisting suicide
- Offences relating to sexual images i.e., revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences - harassment and stalking
- Drug-related offences
- Weapons / firearms offences
- Fraud and financial crime including money laundering
- activities that might be classed as cyber-crime under the Computer Misuse Act (1990)

Other Incidents
Whilst the school would hope that all users would be responsible users of digital technologies, who understand and follow school policy, there may be times when incidents may happen. In the event of suspicion, the following should happen:

- Two members of staff will support, to protect individuals if accusations are subsequently reported.
- Review the issue using a computer that will not be used by a student and can be taken off site should the police need to be involved and remove the devise. The same computer will be used for all steps taken for continuity.
- The staff involved in this process will be provided with appropriate internet access. All sites and content visited will be monitored and recorded.

- The URL of any site showing alleged misuse will be recorded, along with the detail of the content of concern. This may require screen shots to be taken. To safeguard the investigators, these may need to be printed and signed – although that would not be the case in child sexual abuse.
- Once this process has been completed, the team will judge if there is a concern or not. If it is decided that it is a concern, the following action/s could be instigated:
    - Internal response or discipline procedures
    - Involvement by Local Authority / MAT group
    - Police involvement and/or action
    - If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour or the sending of obscene materials to a child, adult material which potentially breaches the Obscene Publications Act or criminally racist material, promotion of terrorism or extremism, other criminal conduct, activity or materials.
- The computer should be isolated to prevent any hindrance should a police investigation be required.
- It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Online Safety Incident Flowchart



Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.

Implement changes.

Monitor situation.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediatelv.

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Await Police response.

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix A – Acceptable User Policy – Staff

All staff are required to read and electronically sign an Acceptable User Policy (AUP) which clearly states the responsibilities of staff using technology in the workplace. This will be signed when they commence their employment at Two Rivers and will be re-enforced monthly.

The AUP list the responsibilities of all staff and covers the use of digital technologies in school: i.e. e-mail, internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Executive Headteacher/Headteacher and the Local Governing Board.
- I will not reveal my password(s) to anyone. I will not log on for another person.
- I will not allow unauthorised individuals to access e-mail / internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I understand that there is a difference between my professional and private roles. I will not engage in any online activity that may compromise my professional responsibilities, this refers to social network sites such as Facebook, Instagram, LinkIn, etc. (Refer to Staff Code of Conduct)
- I will only use the approved, secure e-mail system(s) for school business.
- I will only use the approved school e-mail, school learning platform or other school approved communication systems with students or parents/carers, and only communicate with them on appropriate school business.
- At any time, I will not use school equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or students.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Executive Headteacher/Headteacher.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personally owned digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home. (see Mobile Phones, Camera and Image Policy and Procedures)
- I will use the school's learning platform in accordance with advice.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer, laptop or i-Pad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school if a reasonable amount of personal use outside of school hours becomes "significant personal use" as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is code protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection guidelines require that any information seen by me with regard to staff or student information, held within the school's information

management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage is monitored and that monitoring data could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Appendix B – Acceptable User Policy – Students Two Rivers High School

Two Rivers School provides computers for use by students, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all students and staff and students are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Students are responsible for good behaviour with the resources and on the Internet just as they are in a classroom or a school corridor. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Personal Mobile Devices

- All personal mobile devices should be handed in at reception at the start of the day and not used in classrooms unless authorised by a member of staff.

Equipment

- I understand that damaging the computer equipment intentionally will cut short my time with the ICT equipment.
- The computers should only be used for education purposes unless specified by a member of staff.
- The computers should be protected from spillages by eating or drinking well away from the ICT equipment.
- I will not bring any devices from home and try to connect them to the network unless a member of staff has allowed me to.
- I will immediately report any damage or faults involving equipment or software to a member of staff.

Security and Privacy

- I understand that the school will monitor my use of the systems, devices and digital communications. Staff may review files and communications to ensure I am using the system responsibly.
- I will keep my username and password secure and will not share it, nor will I use someone else's username and password.
- I will be aware of "stranger danger" when I am communicating online.
- I will not disclose or share any personal information about myself online.
- I will immediately report any unpleasant, inappropriate material or messages that make me feel uncomfortable whilst using the ICT equipment.
- I will respect other people's work and will not access, copy or remove any users' files without the owners' knowledge and permission.
- I will not take or distribute images of anyone without their permission.

Internet and Email

- Two Rivers School does not allow the use of social networking sites on the school premises and therefore a student shouldn't try to access any social network site. The law states that no student under 13 should access social network sites.
- I will not try and access any inappropriate or illegal materials.

- I will not download documents including music and videos, if it is protected by copyright.
- Inappropriate content on social networking sites out of school hours will be reported to the Online Safety Lead. School is not obliged to take action over such content, but there may be instances from which wider concerns emerge – in such circumstances school may wish to take advice from the local safeguarding team.
- When a disclosure of cyber bullying is made, school will investigate this further, even where the bullying originates outside the school.
- When using email, be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or disclosing personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detention, suspension, contact with parents and, in the event of illegal activities, involvement of the police.

Student ICT Acceptable Use Policy

Please complete the following sections to show that you have read, understood, and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student:

Name: ____

Signed: ____

Date: ____

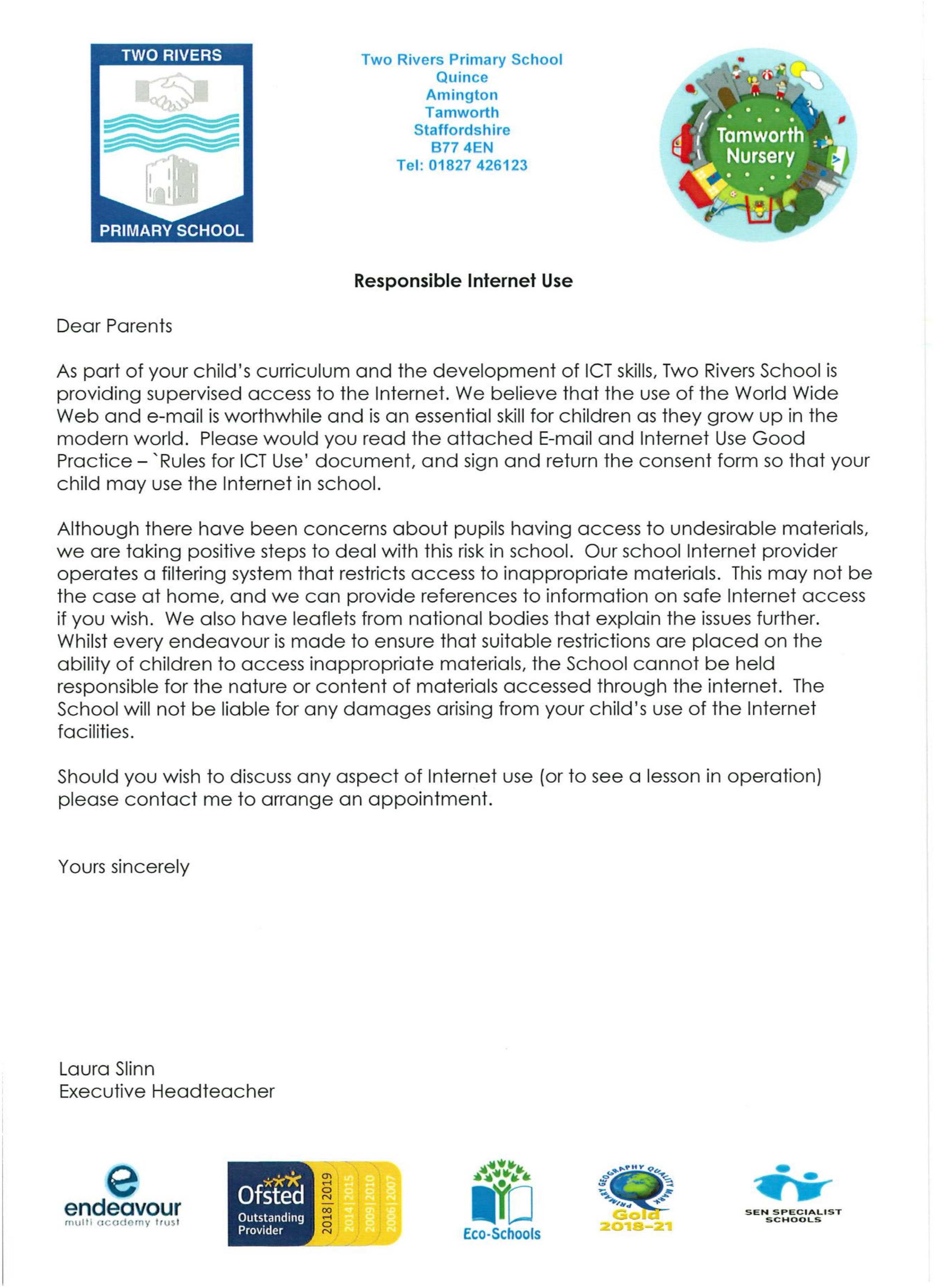
Parent/Person with Parental Responsibility:

Name: ____

Signed: ____

Date: ____

Appendix C – Two Rivers Primary School



Two Rivers Primary School
Quince
Amington
Tamworth
Staffordshire
B77 4EN
Tel: 01827 426123

Responsible Internet Use

Dear Parents

As part of your child's curriculum and the development of ICT skills, Two Rivers School is providing supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached E-mail and Internet Use Good Practice – `Rules for ICT Use' document, and sign and return the consent form so that your child may use the Internet in school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, and we can provide references to information on safe Internet access if you wish. We also have leaflets from national bodies that explain the issues further. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please contact me to arrange an appointment.

Yours sincerely

Laura Slinn
Executive Headteacher

Two Rivers Primary School
Quince
Amington
B77 4EN

Telephone: 01827 426123
E mail: office@tworiversschool.net

Consent Form
Responsible E-mail and Internet Use

Please print Parent/Carers name:

Pupils name:

Parent/Carer's Consent for Internet Access

I have read and understand the school `E-mail and Internet Use Good Practice Rules for ICT Users' in the information booklet and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: **Date:**

Parent/Carer's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed: **Date:**

E mail & Internet Use Good Practice Rules for Students

We use the school computers and Internet connection for learning. These rules will help us to be fair to others and keep everyone safe.

- I will ask permission before entering any website, unless my teacher has already approved the site.
- On a network, I will use only my own login and password, which I will keep a secret.
- I will not look at, change or delete other peoples files.
- I will onlly use the computers for school word and homework.
- The messages I send will be polite and sensible.
- On social media and e mail I will not give my home address or phone number, or arrange to meet someone.

- I will only e mail people my teacher allows.

- I will not use Internet chat.

- If I see anything I am unhappy with or I receive a message I do not like, I will tell and adult immediately.

- I know that the school can check my computer files and will monitor the Internet sites I visit.

- I understand that if i deliberately break these rules, I could be stopped from using the Internet or computers.

The school will exercise its right by electronic means to monitor the use of the schools computer systems, including the monitoring of websites, the interception of email and the deletion of inappropriate materials in circumstances where it believes unauthorised use is taking place, or the system is or may be being used for criminal purposes or for string text or imagery which is unauthorised or unlawful.

Appendix D - Record of reviewing devices/internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Investigating Team	Reviewing Person 1	Reviewing Person 2
Name		
Position		
Signature		

<table>
<tr><td colspan="2">Name and location of computer used for review:</td></tr>
<tr><td>Website addresses / device</td><td>Reason for concern</td></tr>
<tr><td colspan="2">Conclusion and action proposed or taken</td></tr>
</table>