ONLINE SAFETY

STATEMENT OF INTENT

New technologies inspire children to be creative, communicate and learn. However, while the internet is an amazing resource it is also important that children are protected from the risks they may encounter and their online experiences at school are safeguarded.

AIMS AND OBJECTIVES

1.1 Online safety is recognised as an essential aspect of safeguarding pupils and Riverside aims to embed safe practices into the culture of the school. All members of staff have the responsibility for online safety.

1.2 Riverside School aims to:

- have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- uphold the Prevent duties of the school
- deliver an effective approach to online safety, which empowers us to protect and educate the school community in its use of technology
- establish clear mechanisms to identify, prevent, intervene and escalate an incident, where appropriate.

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

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

CONTENT AND PROGRESSION

2.1 The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Link Governor for ICT will co-ordinate regular meetings with appropriate staff to discuss online safety. All governors will ensure that they have read and understand this policy.

2.2 The Designated Safeguarding Leads have the responsibility for online safety in school, in particular:

- supporting the SLT in ensuring that staff understand policies that are being implemented consistently throughout the school
- working with the SLT, ICT technicians and other staff, as necessary, to address any online safety issues or incidents
- ensuring that any online safety incidents are dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with school policy
- updating and facilitating staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing body.

This list is not intended to be exhaustive

2.3 The ICT technician is a representative of **Classroom365** who are responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- conducting a full security check and monitoring the school's ICT systems on a weekly basis
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- ensuring that any online safety incidents are reported to a Designated Safety Lead
- ensuring that any incidents of cyber-bullying are reported to a Designated Safety Lead.

This list is not intended to be exhaustive

2.4 All staff are responsible for promoting and supporting safe behaviours and following school e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

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

- maintaining an understanding of this policy
- implementing this policy consistently
- working with the Designated Safety Leads to ensure that any online safety incidents are dealt with appropriately in line with school policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

ONLINE SAFETY CURRICULUM

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

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

3.2 In **Key Stage 2** pupils will be taught to:

- use technology safely, respectfully and responsibly;

- recognise acceptable and unacceptable behaviour;
- identify a range of ways to report concerns about content and contact

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

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

Online safety measures in place

4.1 To ensure the network is used safely:

- we ensure staff have access to the school's online-safety Policy;
- we ensure staff, pupils, volunteers and parents have signed the acceptable use agreement;
- staff are set-up with Internet and email access and are given an individual network log-in username and password;
- we provide pupils with an individual network log-in username;
- It is made clear that staff must keep their log-on username and password private and must not leave them where others can find;
- we explain to pupils that they should never log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- it is understood that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- we have set up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- all users are required to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- we have set-up the network so that users cannot download executable files/ programmes;
- there is blocked access to music download or shopping sites – except those approved for educational purposes;
- all mobile equipment has anti-virus/spyware software installed before it is connected to the network;
- staff and parents are clear that they are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional/school responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- staff are aware that they are wholly responsible for insurance should portable equipment be taken off site;
- equipment is maintained to ensure Health and Safety;
- there are integrated curriculum and administration networks set up, but access to the Management Information System is set up so as to ensure staff users can only access modules related to their role;

- we only allow **Classroom365** to access our network remotely;
- we use the DfES secure s2s website for all CTF files sent to other schools;
- we ensure all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- we follow LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- the school ICT systems are reviewed regularly with regard to security;
- we do not publish personal e-mail addresses of pupils or staff on the school website;
- we do not post recordings of pupils or staff on the school website;
- parents do not have authorisation to post any recordings or photos taken on the school premises to any internet sites, including social media;
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police;
- accounts are managed effectively, with up to date account details of users;
- pupils only use the school domain e-mail accounts on the school system;
- staff only use the LGfL/school domain e-mail accounts on the school system;
- pupils are introduced to, and use e-mail as part of the Computing scheme of work;

Online Safety training

5.1 **Pupils are taught about safety when using the internet and e-mail i.e.:**

- not to give out their e-mail address without adult consent;
- that any e-mail/message sent should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others, such as address, telephone number, etc;
- to ‘Stop and Think Before They Click’ and not open attachments/sites unless sure the source is safe;
- the sending of attachments should be limited;
- that they must immediately tell a teacher if they receive an e-mail/message which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails/messages, but to keep them as evidence of bullying and report them immediately to an adult;
- not to arrange to meet anyone they meet through the internet or e-mail without having discussed with an adult and taking a responsible adult with them;
- that forwarding ‘chain’ e-mail letters is not permitted.

5.2 **Staff are advised:**

- to use school e-mail system for professional purposes;
- that access in school to external personal e-mail accounts/sites may be blocked;
- of their responsibilities to uphold school policies, including the Behaviour and Prevent policy;
- that e-mail sent to an external organisation is written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school guidelines that:
    - the sending of attachments should be limited;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed.

5.3 **Parents are advised:**

- through parents' training events;
- of internet safety in letters, on the school website or other communications home;
- that any queries or concerns should be raised in the first instance to a Designated Safety Lead or a senior manager;
- that any concerns or queries about this policy can be raised with the SLT.

Unsuitable Material

6.1 We take all reasonable precautions to ensure online-safety and uphold our Prevent duty. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school does not accept liability for material accessed, or any consequences of Internet access but takes every step to prevent this occurring.

Cyber-bullying

7.1 Cyber-bullying takes place online and like other forms of bullying is repetitive, intentionally harming and where the relationship involves an imbalance of power.

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

7.3 The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what consequences can be. Class teachers will discuss cyber-bullying with their class.

7.4 Teaching staff will take opportunities to cover cyber-bullying in PSHE education and other subjects where appropriate.

7.5 All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

7.6 The school sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support their children who may be affected.

7.7 In relation to a specific incident of cyber-bullying, the school will follow school policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

7.8 The SLT will consider whether the incident should be reported to the Police if it involves illegal material and will work with external services, including the Prevent officer, if it is deemed necessary to do so.

Examining Electronic Devices

8.1 School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' personal electronic devices, including mobile phones, iPads/other tablet devices, where they believe there is a 'good reason' to do so.

8.2 When deciding whether there is 'good reason' to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- cause harm and/or

- disrupt teaching and/or
- break any school rules.

8.3 If inappropriate material is found on the device, it is the responsibility of a senior manager to decide whether they should:

- delete that material
- retain it as evidence (of a criminal offence or a breach of school policy)
- report it to the Police.

8.4 Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation and the school's COVID-19 risk assessment.

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

Misuse of ICT

9.1 Staff and pupils are aware of their responsibilities when using ICT. There are sanctions available should there be any instances of misuse, including:

- informing parents or carers;
- removal of Internet or computer access;
- referral to LA/Police.

9.2 The SLT act as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints related to child protection are dealt with in accordance with school/LA child protection/safeguarding procedures.

What we do if….

10.1 All these incidences must be reported immediately to the SLT.

An inappropriate website is accessed <u>unintentionally</u> in school by a teacher or child.

1. Report to the SLT who will decide whether to inform parents of any children who viewed the site.
2. The SLT will inform the school technicians and ensure the site is filtered. (LGfL schools report to: **webalerts@synetrix.com**)
3. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed <u>intentionally</u> by a child.

1. Apply agreed sanctions.
2. SLT to notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

An adult uses School IT equipment inappropriately.

1. Ensure you have a colleague with you; do not view the misuse alone.
2. Report the misuse immediately to the SLT and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the SLT will then:
   - Remove the PC to a secure place.
   - Instigate an audit of all ICT equipment by the school's ICT managed service providers to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action through the governing body.
4. In an extreme case where the material is of an illegal nature:
   - Remove the PC to a secure place and document what you have done.
   - Contact the local police and follow their advice.

A cyberbullying incident directed at a child or member of staff occurs through email, mobile phone technology or website (including social websites), either inside or outside of school time.

1. Advise the child/member of staff not to respond to the message.
2. Apply appropriate sanctions.
3. Secure and preserve any evidence.
4. Inform the sender's service provider.
5. Notify parents of the children involved.
6. Inform the police if necessary – cyberbullying is a criminal offence.

Malicious or threatening comments are posted on an Internet site, including social media, about a pupil or member of staff.

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at www.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (including social networking sites) to make inappropriate contact with the child.

1. Report to and discuss with the Designated Safeguarding Lead in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and social services.
5. Consider delivering a parent workshop for the school community.

10.2 **Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.**

Advice for members of Staff:

11.1 When publishing information about yourself or having one-to-one conversations with others online or by telephone, you are acting at all times as a member of Riverside staff.

11.2 When publishing information, a member of staff will not include personal contact details, video or images or any information regarding any Riverside personnel (adults and pupils) and/or their families.

11.3 Restriction to access to accounts is advisable in all circumstances. Pupils must not be "friends" or be added to contact lists.

11.4 Mobile phones are not to be used on site. Phones must be switched off and locked away whilst on school premises, unless in exceptional circumstances permission is given by the SLT.

11.5 Staff should not phone or email parents or school agencies through their personal accounts unless in an emergency response situation.

11.6 Staff must not take photos of pupils or staff on mobile phones (or with a digital camera that is not a school camera). Photos must never be used on the Internet without prior permission. Past photos should be removed if taking cameras off-site.

11.7 Personal telephone numbers should not be given to parents or pupils. Text messages regarding pupils and their families must not be sent via a personal telephone.

11.8 Confidential information must never be shared electronically.

11.9 Be aware of any information kept on memory sticks and other storage devices, particularly when transporting off-site – security of sensitive information, including photos and names of pupils, is the responsibility of school staff and must be secure and password protected at all times.

11.10 **If for any reason an incident occurs that in any way breaches the content of this advice the person involved must notify the SLT immediately.**

RESOURCES

Acceptable use of the internet in school

12.1 All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

12.2 Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

12.4 We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Riverside

EYFS/KEY STAGE ONE

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (computers/iPads) and get onto the internet in school I will:

Ask a teacher or adult if I can do so before using them

Only use websites that a teacher or adult has told me or allowed me to use

Tell my teacher immediately if:

- ○ I click on a website by mistake
- ○ I receive messages from people I don't know
- ○ I find anything that may upset or harm me or my friends

Use school computers for school work only

Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly

Only use the username and password I have been given

Never share my password with anyone, including my friends

Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer

I agree that the school will monitor the websites I visit.

Signed (pupil):	**Date:**

Parent/carer agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Riverside

KEY STAGE TWO

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (computers/iPads) and get onto the internet in school I will:

Always use the school's ICT systems and the internet responsibly and for educational purposes only

Only use them when a teacher is present, or with a teacher's permission

Keep my usernames and passwords safe and not share these with others

Keep my private information safe at all times and not give my name, address or telephone number to anyone without permission from my parent/carer

Tell an adult immediately if I find any material which might upset, distress or harm me or others

Always log off or shut down a computer when I've finished working on it

I will not:

Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity

Use any inappropriate language when communicating online, including in emails

Create, link to or post any material that is offensive, obscene or otherwise inappropriate

Log in to the school's network using someone else's details

Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone into school:

I will hand it in to the office at the beginning of the school day and collect it at the end of the school day.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):	**Date:**

Parent/carer's agreement:

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**

Riverside

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use the school's ICT systems in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils unless they are linked to an educational activity
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Save school data onto my private home device when accessing the school network remotely

I will only use the school's ICT systems and access the internet in school, or outside school, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and the SLT know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

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