E-SAFETY

INTRODUCTION

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.

RATIONALE

1.1 The school's safeguarding outcomes include our commitment that children and young people are:

- safe from maltreatment, neglect, violence and sexual exploitation;
- safe from accidental injury and death;
- safe from bullying and discrimination;
- safe from crime and anti-social behaviour in and out of school;
- safe from radicalisation;
- secure, stable and cared for.

1.2 These aims apply equally to the 'virtual world' that children and young people will encounter whenever they use ICT in its various forms. For example, we know that the Internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime/anti-social behaviour and/or extremist behaviour.

1.3 It is the duty of our school to ensure that every child in their care is safe, and the same principles should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

1.4 This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- teaching online safety in schools
- preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- searching, screening and confiscation

1.5 It also refers to the DfE's guidance on protecting children from radicalisation.

1.6 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' own electronic devices where they believe there is a 'good reason' to do so.

1.7 The policy also considers the National Curriculum computing programmes of study.

AIMS

2.1 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.

ROLES AND RESPONSIBILITIES

3.1 E-Safety is recognised as an essential aspect of safeguarding pupils and the Headteacher, with the support of Governors, aim to embed safe practices into the culture of the school. All members of staff have the responsibility for e-Safety.

The **e-Safety Co-ordinators** are the **Designated Safety Leads** of the school.

3.2 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.

3.3 The Designated Safety Leads have the responsibility for online safety in school, in particular:

- supporting the Headteacher and Head of School in ensuring that staff understand policies that are being implemented consistently throughout the school
- working with the Head of School, 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

3.4 The ICT technician is a representative of **IES Educational Services Ltd.** 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

3.5 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.

3.6 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.

E-SAFETY CURRICULUM

4.1 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.

4.2 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

4.3 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.

PROCEDURE

E-safety measures in place

5.1 To ensure the network is used safely:

- we ensure staff have access to the school's e-safety Policy;
- 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 **ICT Educational Services Ltd** 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;
- we use e-mail addresses that do not contain children's names throughout the school.

E-safety training

6.1 **Pupils are taught about the safety and 'netiquette' of using the internet and e-mail i.e.:**

- not to give out their e-mail address without adult consent;
- that an e-mail/message is a form of publishing where the message should be clear, short and concise;
- 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/mesages, 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.

6.2 **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.

6.3 **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 Head of School.

Unsuitable Material

7.1 We take all reasonable precautions to ensure e-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

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

8.2 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.

8.3 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.

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

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

8.6 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.

8.7 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.

8.8 The Head of School 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

9.1 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.

9.2 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.

9.3 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.

9.4 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.

9.5 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

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

- interview/counselling by an e-Safety Co-ordinator and/or Headteacher;
- informing parents or carers;
- removal of Internet or computer access;
- referral to LA/Police.

10.2 The e-Safety Co-ordinators 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….

11.1 All these incidences must be reported immediately to the Headteacher or e-safety co-ordinators:

An inappropriate website is accessed unintentionally in school by a teacher or child.

1. Play the situation down; don't make it into a drama.
2. Report to the e-safety co-ordinators who will decide whether to inform parents of any children who viewed the site.
3. The e-safety co-ordinator will inform the school technicians and ensure the site is filtered. (LGfL schools report to: **webalerts@synetrix.com**)
4. Inform the LA if the filtering service is provided via an LA/RBC.

An inappropriate website is accessed intentionally by a child.

1. Apply agreed sanctions.
2. A senior manager 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 a senior manager and ensure that there is no further access to the PC or laptop.
3. If the material is offensive but not illegal, the senior manager 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.
7. Inform the LA e-safety officer.

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.
5. Inform LA e-safety officer.

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 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. Inform LA e-safety officer.
6. Consider delivering a parent workshop for the school community.

11.2 **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

12.1 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.

12.2 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.

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

12.4 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 Headteacher or Deputy Headteacher. Mobile phones that may be used are recorded and the list kept by **Helen Baldry** and **Jill Lewis**.

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

12.6 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.

12.7 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.

12.8 Confidential information must never be shared electronically.

12.9 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.

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

ADVICE FOR PUPILS

13.1 Mobile phones must be given to a senior manager at the start of the day. It is the responsibility of pupils to collect their phone at the end of the day.

13.2 Never give your contact details (such as personal email address or telephone number) to a member of staff or anyone you do not trust.

13.3 You must never use a photo of another child on the internet without their parents' permission.

13.4 You must never send or post an offensive message to a child or adult.

13.4 **You must report anything to an adult, either in school or at home, if there is anything you feel uncomfortable about when using ICT, including using a mobile phone**.