ICT – E-SAFETY POLICY

INCLUDING CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA

This Policy which is applicable to the whole school is part of our Safeguarding – Child Protection Procedures It is publically available on the School website and a copy may be obtained from the School Office.

Monitoring and Review: This policy will be subject to continuous monitoring, refinement and audit by Director of Education Tayyaba Ahmed. The Proprietor will undertake a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than **September 1st 2024**, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed:

Date: 08.01.2024
Renewal: August 2024

Tayyaba Ahmed
Director of Education

Dominic Macauley
Proprietor

Introduction

The primary purpose of this Policy is to safeguard pupils and staff at Riverbank Primary School. It details the actions and behaviour required from pupils and members of staff in order to maintain an e-safe environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to e-safety. Our key message to keep children and young people safe is to be promoted and should be applied to both online and offline behaviours. We filter inappropriate content and teach pupils about staying safe including online harm.

Within our e-safety policy, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main Safeguarding-Child Protection Policy (please refer to our safeguarding policy cited in related documents). Also see related documents to this E-safety policy.

This policy informs and supports a number of other school policies, including our Child Protection Policy and Peer on Peer abuse policy. All staff should read these policies in conjunction with the E-Safety Policy. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Child Protection and Preventing Extremism Policies.

Roles and responsibilities

Our nominated e-Safety Officer is Director of Education Tayyaba Ahmed. He has responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice. This role overlaps with that of the Designated Safeguarding Lead (DSL) role and he works alongside the Deputy DSLs in all matters regarding safeguarding and E- safety.

Their role will include ensuring:

- ensuring young people know how to use the internet responsibly and that parents and teachers have the right measures in place to keep children safe from exploitation or radicalisation;
- all staff and volunteers will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures;.
- clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with pupils. Such policies and procedures are to include the personal use of work-related resources;
- the AUP is to be implemented, monitored and reviewed regularly, and for ensuring all updates are to be shared with relevant individuals at the earliest opportunity;
- monitoring procedures are to be open and transparent;
- allegations of misuse or known incidents are to be dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable;
- effective online safeguarding support systems are to be put in place, for example, filtering controls, secure networks and virus protection;
- an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same
  - this will depend on, for example, the position, work role and experience of the individual concerned and
- a current record of all staff and Pupils who are granted access to school ICT systems is maintained.

Staff Use of IT Systems

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. Recreational or personal use of the Internet and e-mail system is not permitted except with the prior written approval of the Head.

In addition:

- All staff will receive annual update e-safety training.
- All staff must read and confirm by signature that they have read the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- The internet can be used actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to follow the "How do I stay secure on the Internet?" section in the E-Safety FAQ document.

Pupils Use of IT Systems

All pupils must agree to the IT Acceptable Use Policy before accessing the school systems. Pupils at Riverbank Primary School will be given supervised access to our computing facilities and will be provided with access to filtered internet (see FAQ Document) and other services operating at the School. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of children and young people. The school will ensure that the use of Internet derived materials by staff and Pupils complies with copyright law. Riverbank Primary School will help children to understand the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also embedded in our PSHE and SMSC provision. The

latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)

Communicating and educating parents/carers in online safety

Parents will be provided with a copy of the IT User Acceptance Policy, and parents will be asked to sign it on their child's behalf. Riverbank Primary School recognises the crucial role that parents play in the protection of their children with regards to online safety. The school organises annually an awareness session for parents with regards to e- safety which looks at emerging technologies and the latest ways to safeguard children from inappropriate content. Parents and carers are always welcome to discuss their concerns on e-Safety with the school, who can direct them to the support of our e-Safety officer if required.

Protecting Personal Data:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. The school is registered with the Information Commissioners Officer and recognises that if required, data may need to be obtained by relevant parties such as the Police etc.

Radicalisation and the Use of Social Media to encourage extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;

accessing to likeminded people where they are not able to do this off-line, creating an online community;

- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve
  problems and address grievances.

Riverbank Primary School has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils
- Pupils, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools.'*

Reporting of e-Safety issues and concerns including concerns regarding Radicalisation

Riverbank Primary School has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the e-safety officer who will review the issue and take the appropriate action. For pupils, they are taught to raise any concerns to their class teacher who will then pass this on to the e-safety officer. Complaints of a child protection nature must be dealt with in accordance with our child protection procedure.

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Riverbank Primary School ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of children and know where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the e-Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Emerging technologies will be examined by the Director for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered Wi-Fi access.

Cyber-Bullying

Cyberbullying is bullying using technology to threaten, embarrass or cause discomfort. Seven categories of cyber- bullying have been identified:

- **Text message bullying** involves sending unwelcome texts
- **Picture/video-clip bullying via mobile phone cameras** with images or video clips usually sent to other people.
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible.
- **Email bullying** often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to pupils or young people.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online;
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying

ICT based sexual abuse

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Chat Room Grooming and Offline Abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Taking and Storing Images of children including Mobile Phones (See our related documents)

Riverbank Primary School provides an environment in which children, parents and staff are safe from images being recorded and inappropriately used in turn eliminating the following concerns.

- Staff being distracted from their work with children.
- The safeguarding of children from inappropriate use of mobile phone cameras and other digital recording equipment.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image
e.g. mobile phone, tablet, laptop etc.

The school has a Mobile Phone Policy which includes:

- the commitment to keep the children safe;
- how we manage the use of mobile phones at Riverbank Primary School taking into consideration staff, pupils on placement, volunteers, other professionals, trustees, visitors and parents/carers;
- how we inform parents/carers, visitors and other professional of our procedures;
- what type of mobile phones will be used on educational visits and learning outside the classroom;
- The consequences of any breaches of this policy;
- Reference to other policies, such as whistleblowing and safeguarding children policies.

For further information relating to E-safety procedures, refer to the E-Safety Frequently Asked Questions (FAQ) document. It covers the following topics.

- How will the policy be introduced to Pupils? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?
- Why is the use of Internet and ICT important? How is the Safe Use of ICT and the Internet Promoted? How does the Internet and use of ICT benefit education in our school? How will Pupils learn to evaluate Internet content?
- How is Filtering Managed? How is Emerging Technologies Managed? How to React to Misuse by Children and Young People
- How is Printing Managed? What are the categories of Cyber-Bullying? General Housekeeping. What are the Pupil Rules?
- What has Research into Cyber Bullying Found? What is the impact on a child of ICT based sexual abuse? What is the impact on a child of ICT based sexual abuse? How do I stay secure on the Internet? Why is Promoting Safe Use of ICT Important? What does the school's Mobile Phone Policy Include?
- Where can we learn more about Prevent? What do we have to do?
- Do we have to have a separate *Prevent* policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?
- What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Related documents:

- Safeguarding - Child Protection Policy; Anti-bullying Policy; Behaviour and Discipline Policy;
- Prevent Duty: Tackling Extremism and Radicalisation Policy, Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE); The School Rules;
- Taking and storing images of Children – Including Mobile Phones Policy; Acceptable use of ICT Sign off forms for Staff/Students; Use of Photographs Sign-off Form
- What to do if you are worried; www.thinkyouknow.co.uk

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Children Safe in EDUCATION* (KCSIE) *Information for all school and colleges* (DfE: Sep 2023) incorporates the additional statutory guidance and refers to non-statutory advice for practitioners, *What to do if you're worried a child is being abused* (HM Government: March 2015)
- *Working Together to Safeguard Children* (WT) (HM Government: 2015) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Heads and School staff 'and 'Advice for parents and carers on cyberbullying'

- Prepared with reference to DfE Guidance (2014) Preventing and Tackling Bullying: Advice for school leaders and
- governors and the relevant aspects of Safe to Learn, embedding anti-bullying work inschools.
- Having regard for the guidance set out in the DfE (Don't Suffer in Silence booklet)
- The Data Protection Act 1998; BECTA and CEOP.