E-Safety Policy

Policy Details

Policy Level	School
Document Approver	Executive Leadership Team
Document Status	Final
Applicable to	Rugby Free Primary School
Review Frequency	Every 2 Years

Revision History

Revision	Date	Details	Approved by
0	22 May 2024	First Issue	Exec Team

Contents

1. Introduction 3
2. Responsibilities 4
3. Education and Curriculum 6
4. Expected Conduct and Incident Management 8
5. Managing the Computing Infrastructure 10
6. Equipment and Digital Content 13

1. Introduction

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Rugby Free Primary School with respect to the use of computing-based technologies.
- Safeguard and protect the children and staff of Rugby Free Primary School and comply with GDPR (General Data Protection Regulation).
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal, or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Content

- Ignoring age ratings while playing online games (Exposure to Violence associated with often racist/foul language, addiction, in-app purchases)
- Exposure to inappropriate content, including online pornography
- Ignoring age restrictions on social networking websites such as Instagram, Facebook, Tik Tok, You Tube, Snapchat, WhatsApp, and other Apps.
- Data Breach
- Hate sites, sites inciting radicalization and/or extremism
- Content Validation: how to check authenticity and accuracy of online content Contact
- Grooming
- Cyber-Bullying in all forms
- Identity theft and sharing passwords

Conduct

- Privacy Issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and Well-being (amount of time spent online internet or gaming)
- Copyright (little care or consideration for intellectual property and ownership – such

as music and film)

2. Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

PCAB Member for Computing: The role will include

- Regular meetings with the Computing Lead
- Regular monitoring of online safety incident logs (with the Headteacher/Computing Lead)
- Regular monitoring of filtering (with the Headteacher/Computing Lead)
- Reporting to PCAB Meetings.

The PCAB are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the Policy. They will receive regular information about online safety incidents and monitoring reports.

Safeguarding Trustee is responsible for monitoring incidents linked to e-safety on CPOMS. Ensuring that the school has put appropriate actions in place should there be a rise in e-safety incidents.

Head teacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be shared with the Online Safety Co-Ordinator.
- The Headteacher and 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 Headteacher is responsible for ensuring that the Online Safety coordinator receives suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Coordinator.

The Computing Lead:

- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff
- Liaises with school technical staff has a leading role in establishing and reviewing the school online safety policies / documents (in coordination with the Headteacher)
- Meets with PCAB member for Computing to discuss current issues, review incident logs and filtering

- Reports regularly to Senior Leadership Team

Network Manager:

The Network Manager is administered through an IT company (Colwyn Tech) and is responsible for ensuring:

- That the school's '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 other relevant body Online Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis
- 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 / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, Online Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
- They have read, understood, and signed the Staff Acceptable Use Policy Agreement
- They report any suspected misuse or problem to the Headteacher/Computing Lead for investigation/action/sanction
- All digital communications with pupils/parents/carer should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the Online Safety Policy and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils 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

Designated Safeguarding Lead:

- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Pupils are, as in accordance with their age;

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- 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 and Carers

- Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, websites, and information about national/local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:
- Digital and video images taken at school events
- Behaviour and conduct used on school approved platforms (e.g., school social media page, Seesaw)
- Age restricted content

3. Education and Curriculum

Pupils

This school has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHCE curriculum. It is built on Purple Mash scheme of computing learning from EYFS to Y6/ including any national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy;
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- Digital leaders (E-Safety team Ambassadors) are appointed for year 1-5;
- To know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- To understand acceptable behaviour when using an online environment / email, i.e., be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs, and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post photos or videos of others without their permission; to know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyberbullying, sexting, and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e., parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- To know to keep passwords private and that these should not be shared or saved

The school also

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign/will be displayed throughout the school/will be displayed when a pupil logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in popups; buying on-line; on-line gaming / gambling;
- Ensures staff have had GDPR training and know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues, GDPR and the school's e-safety education program; Termly updates in staff meetings.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school runs a rolling programme of advice, guidance and training for parents to ensure that principles of e-safety behaviour are made clear, including:

- Information leaflets; in school newsletters; on the school web site;
- Offer support including demonstrations and workshops sessions held at school;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.

4. Expected Conduct and Incident Management

Expected conduct in this school, all users:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to agree before being given access to school systems
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras, and hand-held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying

Staff

- Are responsible for reading the school's e-safety policy and using the school computing systems, accordingly, including the use of mobile phones, and hand-held devices.
- Are responsible for keeping pupil data secure so that it is GDPR compliant
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse
- At the end of assembly and performances (when invited in) parents/carers are permitted to take photos of their own child/children only and that the school requests that photos/videos are not shared on any social networking site such as Facebook, WhatsApp, snapchat, X (formally known as twitter) etc.

Incident Management in this school:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g., regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors /the LA
- Parents/carers are specifically informed of e-safety incidents involving young people

for whom they are responsible.

- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Data breaches are reported to our Data Protection Champion – The Schools Operation Manager.
- Any E-safety incidents are reported to one of the Designated Safeguarding Leaders through use of CPOMs in accordance with Safeguarding Policy. All staff have had training on this system and have individual logins. If it is a visitor or volunteer, then they can fill in a green form. E-safety incidents are also shared with the E-safety lead so they are aware of incidents that happen in school which may need to change/adapt policies, user logins, training etc.

5. Managing the Computing Infrastructure

Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband connectivity through Smoothwall
- Uses Smoothwall filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age/stage of the pupils;
- Ensures network healthy through use of anti-virus software etc. and network set-up so staff and pupils cannot download executable files;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with Smoothwall and to ensure any concerns about the system are communicated so that systems remain robust and protect pupils;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and pupils have agreed to an acceptable use agreement form and

understands that they must report any concerns;

- Requires staff to plan the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search, ….
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the [system administrator/teacher/person responsible for URL filtering]. Our system administrator(s) logs or escalates as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are, GDPR compliance and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff, and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- Computing devices provided by school to members of staff are regularly checked by the IT technicians.

Network management (user access, backup)

- The trust employs its own technicians. They are to ensure that:
- Users have year group logins for pupils and individual logins for staff;
- Storage of all data within the school will conform to the GDPR requirements
- Staff will only use encrypted USB sticks to hold any data about pupils
- To ensure the network is used safely, this school:
- Ensures staff read and sign that they have understood the school's E-safety Policy, Data Protection Policy Following this, they are set up with Internet, email access and network access. Online access to service is through a unique, audited username and password. Guest users do not have access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes and a 2-factor authentication is required on each device
- We provide pupils with a year group network log-in username and password.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Has 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;

- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- When a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; equipment installed and checked by approved IT technicians
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school e.g., teachers access their area / a staff shared area for planning documentation
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses an internal CCTV system and have had set-up by approved partners;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system or securely accessed via The Bromcom system
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school computer systems regularly with regard to health and safety and security.

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

- We require staff to use STRONG passwords to enter our systems and use a 2-factor login system
- We require staff to change their passwords every 90 days.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers Admin staff and senior leadership team
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, office@rugbyfreeprimary.co.uk home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website; We do not use embedded geo-data in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking

- Teachers are instructed not to run social network spaces for pupils to use on a personal basis or to open up their own spaces to their pupils. School staff will ensure that in private use:
- No reference should be made in social media to pupils / pupils' parents/ carers or school staff
- Data about pupil/ staff or parents is not shared on social media
- 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 /academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

School Mobile Devices such as iPad, learning pads and laptops are used on the school network.

- Mobile phones brought into school are entirely at the staff member, pupils & parents,' or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Parents/carers/visitors are not permitted to use their mobile phones/take pictures and/or videos of staff and/or pupils in school or on the school playground.
- Pupil mobile phones, MP3 players, iPads, smart watches, or any other electronic device which are brought into school must be turned off (not placed on silent) and handed in to the office on arrival at school.
- All visitors are requested to keep their phones off or on silent and are requested not to use them on school grounds.
- The recording, taking, and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the head teacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the head teacher is to be able to withdraw or restricted authorisation for use at any time if it is to be deemed necessary.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, or bullying.
- Staff may use their phones during break times. If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.
- Staff mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Staff may only use their phones during break times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft, or damage of personally-owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the head teacher.
- Images and content recorded for twitter updates will be deleted from the school equipment once it is posted.
- Pupils' use of personal devices
- The school strongly advises that pupils' mobile phones/smart watches/tablets/MP3 players should not be brought into school. The school takes no responsibility for loss or damage of any personal devices brought to school.
- The school accepts that there may be particular circumstances in which a parent

wishes their child to have a mobile phone for their own safety.

- If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Pupil mobile phones/smart watches/tablets/MP3 players should be handed to the school office upon arrival. Pupils found in possession of a mobile phone and or smart watch during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences. However, in case if a pupil has sent an inappropriate message or photo to another pupil at any time and the matter is brought to the attention of the school then the device will be confiscated. Parents/carers will be immediately informed.
- Pupils will be provided with school I Pads/cameras/notebooks/laptops to use in specific learning activities under the supervision of a member of staff. Such devices will be set up so that only those features required for the activity will be enabled.
- No pupils should use his or her mobile phone or personally-owned device in school. Any personal devices used in school by a pupil will be confiscated.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must not be used during lesson times. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families outside of the setting in a professional capacity unless on a school trip.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.

- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then they should hide their caller identification. They can do so by inputting 141 to hide their own mobile number for confidentiality purposes.
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Photos/videos taken on school iPads are stored on the school network.
- Pupils are taught about how images can be manipulated in their e-Safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents, or younger children as part of their Computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse