Policy Name:	ON LINE E-SAFETY	
Policy Author: MR ADAM FARRINGTON HORSFALL	**Linked Governor/reviewer:** MR JOHN HOUGH MR NEIL LOWTHER **Committee:** PUPIL SUPPORT	
Date Approved by Governors: 17.10.16 **Review Frequency: EVERY 3 YEARS OR SOONER AS CHANGES ARE NEEDED**	**Related Policies:** EYFS SAFEGUARDING WHISTLEBLOWING COMPUTING DATA PROTECTION STAFF BEHAVIOUR	
Date for review: 2019 **Document Version: 1**	**Statutory or Voluntary (S/V):**	**V**

Chair of Governors:		**Date:**
Audience:		**Website:**
Pupil Governors	✓	**Yes / No**
Finance/resources Governors		
Standards Governors		
Teaching Staff	✓	
Support Staff	✓	
Lunchtime Staff	✓	
Parents	✓	
Other	✓	

INDEX

1. INTRODUCTION AND OVERVIEW

Return to Index

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at The Richard Clarke First School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of The Richard Clarke First

School.

- 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 students.

The main areas of risk for our school community can be summarised as follows:

- Content
  - exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
  - lifestyle websites, for example pro-anorexia/self-harm/suicide sites
  - hate sites
  - content validation: how to check authenticity and accuracy of online content
- Contact
  - Grooming
  - PREVENT (Online radicalisation)
  - cyber-bullying in all forms
  - identity theft (including 'frape' (hacking Facebook profiles)) 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))
  - SGII (self-generated indecent images) also referred to as sexting (sending and receiving of personally intimate images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.1. Scope

This policy applies to all members of The Richard Clarke First School community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of The Richard Clarke First School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school / academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school / academy, but is linked to membership of the school / academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1.2. Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website / online learning platform / staffroom / classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

1.3. Handling complaints

The school will take all reasonable precautions to ensure e-safety. 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. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by teacher / E-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period;
- referral to local authority / Police.

Our eSafety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / local authority child protection procedures.

1.4. Review and Monitoring

The e-safety policy is referenced from within other school policies: ICT and Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies, Safeguarding policy, Preventing extremism and radicalisation safeguarding policy.

- The school has an e-safety coordinator who will be responsible for document ownership, review and updates.
- The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written by the school e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTFA. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. EDUCATION AND CURRICULUM

Return to Index

2.1 Using ICT in the Classroom

This school has a clear, progressive e-safety education programme as part of the computing curriculum / PSHE curriculum. It is built on local authority e-safeguarding and e-literacy framework from 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;
- 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 online '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 pictures 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;
- To understand the impact of cyber bullying and know how to seek help if they are affected by any form of cyber bullying.

- To know how to report any abuse including cyber bullying; 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.

The school plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which will be displayed throughout the school. Staff will model safe and responsible behaviour in their own use of technology during lessons, and ensures that when copying materials from the web, pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights. The school 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 pop-ups; buying on-line; on-line gaming / gambling;

2.2 Staff and governor training

This school:

- Ensures staff 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
- 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.

2.3 Parent awareness and training

This school:

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

3. EXPECTED CONDUCT AND INCIDENT MANAGEMENT Return to Index

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to accept before being given access to school systems. (in EYFS it would be expected that parents/carers would give acceptance on behalf of the pupils.)
- 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 eSafety 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 ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils 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. They should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

4. MANAGING THE ICT INFRASTRUCTURE

Return to Index

4.1 Internet access, security (virus protection) and filtering

This school:

- Has the educational filtered secure broadband and so connects to the 'private' National Education Network;
- Uses a 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 is logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software etc.
- Uses DfE, or LA approved systems (e.g. school email) to send personal data over the Internet and uses encrypted devices where staff need to access personal level data off-site;
- 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;
- Uses security time-outs on Internet access where practicable / useful;
- 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 students have accepted an acceptable use agreement and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment: e.g. the school's learning environment;

- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. KidRex;
- 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 students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are 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.
- Has weekly reports from online monitoring services about content and websites accessed from any computers connected to the school network.

4.2 Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager has up-to-date policies:

All data storage within the school will conform to UK data protection requirements. Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

4.3 Ensuring that the network is used safely.

This school :-

- Ensures that all staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access.
- Controls staff access to the schools' management information system through a separate password for data security purposes;
- Provides pupils with an individual network log-in username. From Year 3 they are also expected to use a personal password;
- Allocates a unique username and password to each pupil which gives them access to the Learning Platform;

- 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;
- Requires every one, finding a logged-on machine, to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 1800hrs to save energy;
- Makes clear that staff are responsible for ensuring that any device 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.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
    - e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
    - e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers

- 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;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password;
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- 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 the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure 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;
- Makes sure that our wireless network has been secured to appropriate standards, suitable for educational use;

- Makes sure that all computer equipment is installed professionally and meets health and safety standards;
- Maintains projectors so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

4.4 Password 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 it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

4.5 E-mail Accounts

This school:

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LA technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, Securus filtering monitors and protects our Internet access to the World Wide Web.

Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, and we explain how any inappropriate use will be dealt with.

4.6 Staff use of e-Mail

All staff sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

- Staff only use LA e-mail systems for professional purposes
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;

4.7 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- 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. 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 expect teachers using school approved blogs or wikis to password protect them and run from the school website.

4.8 Learning platform (LaunchPad)

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's learning platform will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the learning platform;

4.9 Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The school's preferred system for social networking will be maintained in adherence with the communications policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

5. DATA SECURITY: Management Information System (Access & Data transfer)

Return to Index

5.1 Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.
- We ensure ALL the following school stakeholders understand the relevant Acceptable Use Policy.

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any protect and restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

5.2 Technical Solutions

- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- The server is in the admin office managed by DBS-checked staff.
- We use backups for disaster recovery on our server.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

6. EQUIPMENT AND DIGITAL CONTENT

Return to Index

6.1 Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at individuals own risk. The

School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- Student mobile phones must not be brought into school.
- All visitors are requested to keep their phones on silent.
- 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 Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict 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 mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. 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.
- 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.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

6.2 Students' use of personal devices

- The school does not allow student mobile devices to be brought into school. Any devices that are will be confiscated and returned to an adult at the end of the day.

6.3 Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model. 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 within or outside of the

setting in a professional capacity. Staff are to use the school phone where contact with students, parents or carers is required.

- 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.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose, without prior approval from the senior leadership team.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

6.4 Digital images and video

In this school:

- 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 / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- 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;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also 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 the identify 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.

6.5 Asset disposal

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen. Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.