THE ROSEWOOD SCHOOL

Staff Responsible Name: Mr D Kirk Policy Date – September 2023 Review Date – September 2024



School E-Safety Policy 2023-2024

 **School E-safety policy – Written in due regard to KCSiE 2023**

1. Introduction
	1. The internet and e-mail play an essential role in the conduct of our business in school. The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.
	2. How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail and the internet.
	3. We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.
	4. For your safety, we are able to monitor all web pages visited, email sent and received, this helps us monitor inappropriate use, such as bullying.
	5. This policy applies to you as an employee whatever your position, whether you are a Head Teacher, Teacher, support staff, permanent, temporary or otherwise. Any inappropriate use of the School’s internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.
	6. It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher
2. GENERAL PRINCIPLES and legal issues
	1. All information relating to our pupils, parents and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically.
	2. Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.
	3. We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.
	4. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However the same principles apply to information exchanged electronically in this way as apply to any other means of communication. For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
	5. Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher.
	6. As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.
	7. All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.
3. MONITORING COMMUNICATIONS
	1. This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

 3.1.1 To establish the existence of facts

 3.1.2 To ascertain compliance with applicable regulatory or self-regulatory practices or procedures.

 3.1.3 To ascertain or demonstrate effective system operation technically and by users.

 3.1.4 For national security/crime prevention or detection.

 3.1.5 For confidential counselling/support services.

 3.1.6 For Investigating or detecting unauthorised use of the system

 3.1.7 For monitoring communications for the purpose of determining whether they are communications relevant to the business.

* 1. Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the right to withdraw from employees the facility to send and receive electronic communications
	2. If the email is personal, it is good practice to use the word ‘personal’ in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
	3. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School’s business purposes which include the following:
		1. Providing evidence of business transactions;
		2. Making sure the School’s business procedures are adhered to;
		3. Training and monitoring standards of service;
		4. Preventing or detecting unauthorised use of the communications systems or criminal activities;
		5. Maintaining the effective operation of communication systems.
1. USE OF INTERNET AND INTRANET
	1. When entering an internet site, always read and comply with the terms and conditions governing its use.
	2. Do not download any images, text or material which is copyright protected without the appropriate authorisation.
	3. Do not download any images, text or material which is inappropriate or likely to cause offence.
	4. If you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible /RM. They should check that the source is safe and appropriately licensed.
	5. If you are involved in creating, amending or deleting our web pages or content on our web sites, such actions should be consistent with your responsibilities and be in the best interests of the School.
	6. You are expressly prohibited from:
		1. Introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
		2. Seeking to gain access to restricted areas of the network;
		3. Knowingly seeking to access data which you are not authorised to view;
		4. Introducing any form of computer viruses; and
		5. Carrying out other hacking activities.
	7. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:
		1. Unauthorised access to computer material i.e. hacking;
		2. Unauthorised modification of computer material; and
		3. Unauthorised access with intent to commit/facilitate the commission of further offences.
2. USE OF ELECTRONIC MAIL
	1. You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.
	2. Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is ‘Confidential@ in the subject line
	3. Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
	4. Do not impersonate any other person when using e-mail or amend any messages received.
	5. It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
3. DATA PROTECTION
	1. Through your work, personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*’s* premises or working remotely you must:
		1. Keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;
		2. Familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
		3. Familiarise yourself with all appropriate School policies and procedures;
		4. Not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.
	2. The School views any breach of the Data Protection Act 1998 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.
	3. If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.

**Cyberbullying**

Internet, Digital, Safeguarding Policy must be read in conjunction with KCSiE 2023, Anti-bullying policy and Safeguarding and Child Protection policy (including Prevent, online challenges / hoaxes and sexual violence and harassment).

Cyberbullying may be defined as ‘the use of electronic communication, particularly mobile phones and the internet, to bully a person, typically by sending messages of an intimidating or threatening nature’.

Cyber bullying can be received in many forms or threats such as: intimidation, harassment or ‘cyber-stalking’ (e.g. repeatedly sending unwanted texts or instant messages), sexting maliciousness/defamation, exclusion/peer rejection, impersonation, unauthorised publication of private information/images and ‘trolling’ (abusing the internet to provoke or offend others online).

It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

However it differs from other forms of bullying in several significant ways:

• It allows for a far more extreme invasion of personal space. Cyberbullying can take place at any time and intrude into spaces that have previously been regarded as safe and personal (e.g. the person’s home/bedroom)

• It allows for anonymity on the part of the bully.

• It allows the bully to be seen by a larger audience and allows for other peers to join in (child on child bullying), this also allows the scale of the bullying to rapidly become out of control.

• It can affect the victim more knowing that the evidence will always be online.

• There is a difficulty in trying to control electronically circulated messages as more people get drawn in as accessories. By passing on a demeaning picture or text messages, a bystander becomes an accessory to the bullying.

• The profile of the bully and target can be different to other forms of bullying as cyberbullying can take place between peers and across generations. Teachers can be victims and age and size are not important.

• Many cyberbullying incidents can themselves act as evidence so it is important the victim saves the information.

**Preventing Cyberbullying**

As with all forms of bullying prevention is key, there is no-way that the school can monitor pupils’ devices outside of school and at all times in school hours, however; as a school we strive to inform pupils, parents and carers of all the latest online trends, how to block, delete and report and how to notice signs of cyberbullying . There is no single solution to the problem of cyberbullying however we do believe that by doing the following we can minimise the risks:

* Head of ICT **Mrs Amie Cooper with support of the DSL** will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies.

• We will ensure that all incidents of cyberbullying inside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school’s Anti-bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy. We will support parents and give advice in line with the law regarding matters that take place outside of school.

• We ensure that all policies relating to safeguarding, including cyberbullying are reviewed and updated regularly and that we attend meetings / courses to stay abreast of any new ideologies.

• We ensure that all staff know how to report any issues concerning safeguarding including cyberbullying to the Designated Safeguarding Lead or assistant safeguarding leads.

• We ensure that all staff are aware of the Prevent Duties.

• We provide up to date, relevant training so that staff feel confident in identifying children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk.

• We ensure that parents/carers are informed where school policies can be found so that they are fully aware of the school’s responsibility relating to safeguarding pupils and their welfare. All policies are available on the school website or in school and can be requested at any time.

• We send out a copy of the e-safety and cyber bullying leaflet, there are links to this on the school website also.

* We are a registered and accredited National Online Safety School, monthly newsletters are sent out to parents and carers and are available on the school website.

* Cyberbullying is revisited as part of the ICT E-safety Programme each term across all key stages, we partake in debates and e-safety days and pupils are reminded of how to report a concern. (A trusted adult, Child line or the thinkuknow website: <https://www.thinkuknow.co.uk>

• All staff are aware of their responsibilities and are given guidance on the use of technology within school and beyond. All staff should sign to say they have read, received and understood the Staff Code of Conduct, ICT and E-safety policy in line with the schools Safeguarding Policy linked policies. All staff are aware of the latest KCSiE document.

• We ensure that all pupils are given clear guidance on the use of technology in a positive and safe manner both in school and at home, ICT lessons cover how to manage personal data and to report abuse / bullying online.

• We offer courses to parents and offer support to parents and carers where appropriate in developing their skills and understanding in the use of technology.

• We ensure the Acceptable Use Policy and Children’s Use of Digital Devices are reviewed annually and signed to state it has been read, received and understood.

• We ensure that ICT plan’s and deliver’s a curriculum on online safety which helps to build a resilience within the pupils to allow them to protect themselves and others online.

• We ensure appropriate filters are in place to block inappropriate content and use RM to support this.

• School visitors are given clear guidance on the use of technology in school. This includes how to report any safeguarding issues to the Designated Safeguarding Lead. Supply staff are given highly restricted staff accounts which do not allow any access to staff drives or pupil data.

• The school governing body works together to ensure policies and practices relating to safeguarding including the prevention of cyberbullying are being implemented effectively. Safeguarding governor is **Mr Paul Leyshon.**

**All staff are expected to take responsibility for using technology positively.**

* The school will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.
* The school will deal with inappropriate use of technology in the same way as other types of inappropriate behaviour and sanctions will be given in line with the school’s Behaviour Policy.
* It is vital that parents/carers and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying and parents/carers must play their role and take responsibility for monitoring their child’s online life.
* Parents/carers can help by supporting the school and inform their child of how seriously the school takes incidents of cyber-bullying.
* Parents/carers can also help to reinforce prior learning such as the legal issues relating to cyber-bullying.

Several sites offer helpful advice to parents/carers, such as:

• [www.thinkyou.know.co.uk/parents](http://www.thinkyou.know.co.uk/parents)

• [www.saferinternet.org.uk](http://www.saferinternet.org.uk)

• [www.digizen.co.uk](http://www.digizen.co.uk)

• [www.nspcc.org.uk](http://www.nspcc.org.uk)

• [www.childnet.com](http://www.childnet.com)

Or please visit Rosewood’s school website where a link to the National Online Safety support page can be found alongside the monthly newsletters and the schools e-safety leaflet.

We also send out newsletters and text messages to parents/carers inviting them to engage with the free online courses available to them.

All risk assessments and risk registers have been updated in line with KCSiE and Government requirements for filtering and monitoring.