RUPERT HOUSE SCHOOL

E-SAFETY AND IT ACCEPTABLE USE POLICY

Policy Owner – Deputy Head Academic

Management Committee responsible: Senior Management Team

Governor oversight: Education Committee

Approval: Education Committee

Last review date: October 2023

Next review/approval date: October 2024

Contents

1. AIMS AND PURPOSE

Rupert House School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, visitors using our network and governors
- Deliver an effective and positive approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Use the internet and other digital technologies to support, extend and enhance learning

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce:** being exposed to financial or contractual risks, such as online gambling, inappropriate advertising or financial scams

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

This policy applies to all pupils, all teaching staff, all support staff, all Governors, all visitors using our network and all volunteers.

- To educate pupils about e-safety issues and appropriate behaviours so that they remain safe and legal online
- To help pupils develop critical thinking skills to reflect and enable them to keep themselves safe
- To keep personal information secure
- To minimise the risks of handling sensitive information
- To ensure that all members of the school community (including staff, pupils, volunteers, parents / carers, visitors,) benefit from ICT access, with clear guidance on safe and acceptable use.
- To make all members of the school community (including staff, pupils, volunteers, parents / carers, visitors,) aware that ICT use in school is a resource and a privilege. If the terms are not met that the privilege will be taken away.
- Provide guidance to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) about the acceptable use of current technologies.

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 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, but is linked to membership of the school. 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 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.

2. LEGISLATION AND GUIDANCE

This policy is based on the latest version of the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

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

The policy also takes into account the National Curriculum computing programmes of study.

3. ROLES AND RESPONSIBILITIES

3.1 The governing board

The governing board has overall responsibility for holding the Head and SMT to account for the implementation of this policy.

The governor who has oversight of safeguarding is Michelle Brennan. She meets termly with the Designated Safeguarding Lead (DSL) to discuss online safety, and to monitor online activity as provided by the DSL.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Receive appropriate Child Protection training to include online safety training

3.2 The Head

The Head is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our Safeguarding and Child Protection policy.

The DSL and Deputy Head, Academic take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Network manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board at the Risk and Governance committee meetings

This list is not intended to be exhaustive.

3.4 The Network manager

The Network manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a termly full security check and monitoring the school's ICT systems on a daily basis
- Blocking access to potentially dangerous or inappropriate sites and, where possible, preventing the downloading of potentially dangerous or inappropriate files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 The Head of Computing

The Head of Computing is responsible for:

- Taking day to day responsibility for e-safety issues and establishing and reviewing the school's acceptable use policies / documents
- Raising awareness of safe internet use to children, as part of the Computing and PSHE curriculum
- Working with the DSL to organise talks and events for pupils, staff, parents and Governors, on e-safety.

- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Providing training and advice for staff and liaising with the SMT and Network Manager to review policy and procedures
- Using reports of e-safety incidents to inform future e-safety developments

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) and ensuring that pupils follow the school's terms on acceptable use (appendix 1). Nb. Staff will receive online safety information at induction and will also be given regular training updates regarding online safety information.
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure they and their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Have a conversation Childnet International: https://www.childnet.com/parents-and-carers/have-a-conversation/
- National Online Safety E-safety Guides for Schools | National Online Safety

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when connecting to the school's IT system, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Visitors and members of the community using the school's ICT systems or internet are expected to:

- Respect the integrity of our network and any other public or private computing and network systems
- Not use the Guest Wireless Network for malicious, fraudulent, or misrepresentative purposes
- Not use the Guest Wireless Network in a manner that precludes or hampers other users' access to the Guest Wireless Network or other any other networks.
- Not install or use anything that modifies, disrupts, or interferes in any way with service for any user, host, or network.

Any visitor can be disconnected from the network at any time and for any reason, at the discretion of the Head.

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Pupils will be taught about online safety as part of the curriculum.

In **EYFS** and **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour and be made aware of harmful online challenges and hoaxes
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

In addition, the school invites external specialists to reinforce the importance of e-safety to children, parents and staff.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The school raises parents' awareness of internet safety in letters or other communications home, and in information via our website or parent app. This policy is also shared with parents.

Online safety is also covered during a specialist evening for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Head.

6. TRAINING GOVERNORS ON ONLINE SAFETY

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the National Governors Association or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

7. CYBERBULLYING

7.1 Definition

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

7.2 Preventing and addressing cyberbullying

The school must be aware of 'harmful online challenges and online hoaxes' as mentioned in the updated KCSIE 2023.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form and ICT specialist teachers, will discuss cyberbullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHEE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, report the locating of inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. Parents and SMT will be notified in this instance.

When deciding whether there is a good reason to examine data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material
- Report it to the parents
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

8. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

9. PUPILS, STAFF AND VISITORS USING MOBILE DEVICES IN SCHOOL

Pupils are permitted to bring mobile phones into school with permission from the Head but must be left in the school office. In exceptional circumstances, and for health reasons only, a pupil may carry a mobile phone with them around school. This will be carefully monitored by staff.

In Year 6, and with the Head's and parent(s) agreement, pupils are allowed to walk home on their own at the end of the school day. In these instances, they may bring a mobile phone into school. This is on the understanding that they must leave the mobile in the school office at the beginning of the day and collect it before walking home. In order for this to happen, parents must sign a consent form [see *Supervision of Children* and *Collection of children from school* policies].

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff are not permitted to use their personal mobile devices or cameras in the presence of children. If staff need to take photographs for educational purposes, the photographs must be transferred to the relevant location as soon as is reasonably practicable and immediately deleted. Staff who act in breach of this may be subject to disciplinary action.

Visitors, including parents/carers, are not permitted to use their personal mobile devices or cameras in the presence of children, whilst on site. If a visitor or parent/carer is seen using their mobile phone or device, they will be asked to switch it off. The school displays notices advising visitors that mobile phones are not to be used in the setting.

10. STAFF USING WORK DEVICES OUTSIDE SCHOOL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

11. HOW THE SCHOOL WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. MONITORING ARRANGEMENTS

The DSL logs behaviour and safeguarding issues related to online safety using MyConcern.

This policy will be reviewed annually by the SMT and Head of Computing. After every review, the policy will be shared with the governing board at the Education Committee meeting.

14. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct/Handbook
- Data Protection Policy and privacy notices
- Complaints Procedure
- Staff Induction Policy
- Collection of children from school Policy
- Supervision of Children Policy

Appendix 1: acceptable use agreement (pupils and parents/carers)

Acceptable use of the school's ICT systems and internet: agreement for pupils and parents/carers

Name of pupil:

When using the school's ICT systems and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Access any inappropriate websites
- Access social networking
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the school's network using someone else's details
- Give out personal information about myself or others
- Arrange to meet anyone offline

If I bring a personal mobile phone or other personal electronic device into school:

- I will hand it in to the school office and collect it at the end of the day.
- I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and appropriately

I agree that the school will monitor the websites I visit.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I understand that when using the personal electronic device at home I am responsible for keeping my child safe on the internet.

Signed (parent/carer):

Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

October 2023