Subject:	**Online Safety**	Number:	**POL00126**
		Type:	**Policy**
Approved by:		Effective:	**September 2022**
		Revision:	**2**
	Managing Director	Effective:	**September 2023**

1. Objectives

Living in the 21st Century brings a fantastic and amazing digital era right into the palm of our hand. While the Robert Holme Academy recognises that these new technologies can provide positive experiences and opportunities for children and young people to learn, play and socialise, we also understand that we have a responsibility to educate and safeguard our young people against the challenges and risks that they can face in the digital age. The Robert Holme Academy believe that Information and Communications Technology is an essential resource to support learning and teaching for adults and children in both the school and the wider community. Provision and facilities therefore reflect the very latest technology, along with the necessary controls to safeguard our pupils against present-day exposures and vulnerabilities.

It is becoming more and more prevalent that people's future success may depend on them having sensible online skills and upholding their personal and professional reputation in a manner that is fit for the working world. With this in mind, we are committed to ensuring that all students and staff will be supported to use the internet, mobile and digital technologies safely, including supporting parents and carers in keeping their children safe at home.

It is important that all stakeholders understand the impact of their digital footprint, and that it can, and will, be held against them in the future – even if it is something that has been said/done historically.

As a SEND school, we are also aware that some students may require additional support, teaching, prompts, reminders or further explanations to emphasise the importance of online safety issues. However, all pupils, irrespective of their ability and needs, will have access to a range of up to date technologies including PC equipment, tablets, micro-controllers, etc., providing the best opportunities to develop their skills.

We recognise the constant and fast paced evolution of Information and Communications Technology across society as a whole and acknowledge the essential role it plays in support of learning and teaching, as well as being an essential feature in the day to day activities of children, young people and adults.

We understand the responsibility to educate our pupils on e-safety vulnerabilities, while equipping them with appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. Thus, we aim to build on the skills in using these technologies in order to equip our students with the skills to access lifelong learning and employment. However, we will take the necessary precautions to ensure users need to be aware of, and are protected from, the range of risks associated with the use of internet services.

2. *Scope and Applicability*

This policy mandates the practices necessary to promote online safety in all aspects of work at the Robert Holme Academyand is applicable to:

- students;
- teaching and support staff;
- volunteers;
- supply/agency staff;
- visitors; and
- parents/carers.

The policy and procedures identified within this document apply to all use of possible opportunities using Information and Communications Technology and internet. These include, but are not limited to access to:

- websites;
- learning platforms and virtual learning environments
- blogs;
- podcasting;
- video broadcasting;
- music and video content;
- email and instant messaging;
- chat rooms and social networking;
- gaming; etc.

The Robert Holme Academy is committed to providing and guiding parents/carers to online safety information in order to help keep their child as safe as possible online. However, it is important to note that parents/carers must understand that they play a key role in supporting their child to behave and conduct themselves appropriately online, and to explain that actions online can have serious repercussions both now and in the future.

This policy is intended to protect the interests and safety of our whole school community and is supported by the use of acceptable use agreements. We also ensure that keeping our students safe online is embedded into our curriculum explicitly in PSHE, computing and implicitly through the rest of our curriculum, as well as in tutor time, assemblies, anti-bullying policy, child protection and safeguarding policy, data protection, home/school agreement, sex and relationships policy and the health and safety policy.

3. Procedure

3.1 Responsibilities

3.1.1 Responsibilities of the Managing Director

The Managing Director has overall responsibility for maintaining the overall policies for eSafety, while setting the overall strategies for, and provided sufficient resources to maintain, online safety.

In this capacity, the Managing Director will:

- provide the necessary computer facilities and supporting software;
- ensure Information and Communications Technology facilities are up-to-date and fit for purpose, including access to the Internet;
- monitor access to the internet and review computer use;
- take appropriate action where breaches in online safety have occurred;
- take appropriate action equipment is misused, such as to access and/or download illegal content.

The Managing Director also delivers online safety training during the induction program for new members of staff and regular update training/briefings for all members of staff.

3.1.2 Responsibilities of the Headteacher

The Headteacher has a primary responsibility for the implementation of online safety practices and for monitoring their effective implementation on a day-to-day basis. The Headteacher therefore:

- ensures sufficient staff are adequately trained in online safety and related policies, procedures, systems and working practices;
- supervise and monitor access to the internet and computer use;
- ensure staff also supervise and monitor access to the internet and computer use;
- log any violation or breach in online safety in MyConcern and report the issue to the Managing Director;
- ensure staff sign the ICT user agreement

3.1.3 Responsibilities of all Staff

All members of staff have a responsibility for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures. All staff are therefore responsible for making sure that they are aware of, and comply with, online safety policies and procedures.

Staff are responsible for ensuring all school computer equipment, including any personal laptops, or those provided by the school are fully compliant with this policy and are required to surrender any equipment for inspection as required.

Similarly, all staff are encouraged to provide feedback along with recommendations for improving online safety on an ongoing basis.

Staff are also expected to fully commit to any changes in policy, procedure and working practices supporting online safety.

All staff are reminded that it is their responsibility to monitor online usage during their lessons and to report any inappropriate usage via the MyConcern log. All staff are reminded of their professional duty to show and use appropriate online content and material when teaching the children in their classes, or during social times in the school day.

3.2 Use of email

All staff, including the Managing Director, should use their school email account. This is to be used for all official and professional school communication to protect themselves and the integrity of the school. This is to enable all staff to be protected and accountable and ensure the traceability of all communication.

Staff must not contact students, parents/carers or conduct any matters regarding school business using their own personal email address. This is a mandatory requirement and will lead to disciplinary action if this occurs. All contact must be made using school emails, school phone(s) or Class Dojo. Staff must not delete any communication streams

For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for confidentiality and data protection. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

If staff or students receive suspect sources through emails or attachments, they should not open them and report them to the Managing Director for advice.

Any user accessing emails must not send emails that are embarrassing, upsetting, offensive or seen to be part of cyberbullying. Disciplinary action will be taken against any member of staff or a student who is seen to be acting in such a way.

3.3 Visiting online sites and downloading

Before using sites, software and apps in school, or recommending them to students, it is the staff member's responsibility to preview the material prior to use.

If an online service requires a user account to be created and/or personal data shared, staff should discuss this with the Headteacher and/or Managing Director who will approve the service if it is found necessary. All terms and conditions should be read and adhered to. Parental/Carer permission should be sought, where required, as soon as possible and before using the service.

Staff must only use approved systems for creating online content and blogs. If a member of staff wishes to use a system that hasn't already been approved, they must seek approval from the Headteacher and/or Managing Director.

If students are searching for images, this must be done under supervision and search through a safe and filtered search engine.

Users, including members of staff, students and visitors, must not visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative);
- indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative);
- adult material that breaches the Obscene Publications Act in the UK;
- promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation
- promoting hatred against any individual or group from the protected characteristics above;
- promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy;
- any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect.

In addition, users must not:

- reveal or publicise confidential information;
- intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses;
- transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school;
- use the school's hardware and Wi-Fi facilities for running a private business;
- intimidate, threaten or cause harm to others;
- access or interfere in any way with other users' accounts;
- use software or hardware that has been prohibited by the school;

3.4 System Security

The Managing Director is in charge of ensuring the school filters are in place for safer internet browsing. However, all staff are required to monitor student use of IT equipment and internet use at all times.

The school internet has a filtering and monitoring facility which blocks all website access against preset policies. Any inappropriate material, whether it be sexual, violent, extremist, illegal, etc., in nature should be blocked. Unauthorised and/or inappropriate access must be reported to the Managing Director for attention.

Viewing, retrieving or downloading of any material that the school considers inappropriate will result in appropriate disciplinary action.

The school reserves the right to monitor the use of the network, internet and e-mail systems. Disciplinary action will be taken if it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached.

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

The following system security rules are appled:

1. All computers and laptops are password protected, which are changed on a regular basis.
2. Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access.
3. Deliberate attempts are not to be made to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across.
4. School hardware must not be modified in any way.
5. External devices such as printers, mice, headphones, scanners, etc., must be used appropriately.
6. Eating or drinking is not permitted while using computer equipment.
7. Users must log out of any device properly after use and ensure the device is shutdown in order to protect user data.
8. If a person leaves their workstation for any period of time they should log out of their workstation.

The Robert Holme Academy is aware that staff may use a personal device outside of work hours to conduct school business. However, closed, monitorable systems that have been set up by the school should be used, or an encrypted memory stick, to ensure that the user is not saving files locally to their own device which could compromise confidentiality.

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police and/or disciplinary action taken.

The Robert Holme Academy is aware and recognises that, on occasion, certain planned activities in the curriculum will require access to controversial and/or offensive online material, but is beneficial for educational use in that circumstance. In such instances, members of staff are expected to pre-plan for this, ensure it is risk assessed and recorded and permission is granted by the Headteacher.

3.5 Storing images

As part of our Acceptable Use Agreement, photographs and videos are permitted for use within school, in order to evidence and celebrate students' progress and achievements. Photographs will only be taken/used with the written consent of parents/carers which is secured upon entry to the school. Parents/carers can change their consent at any time.

Photographs and images are stored on the school's system/network (including cloud based services) and under no circumstances should be stored on a personal device. Images will be stored in an appropriate area with access granted to approved staff as determined by the Headteacher. Staff and students may have access to photographs and videos taken during a lesson, however, these will be transferred and/or deleted promptly.

In some circumstances, some children may be classed as vulnerable and at risk, so their images cannot be placed online. Likewise, others may not want their image used online. For these reasons, we ask that parents/carers follow the school's Acceptable Use Agreement and do not take or post images of any member of the school community online (including their own social medias), other than their own child.

Images must only be taken/recorded on school equipment and under no circumstances should a member of staff or other professional take images of recordings of students on their own personal devices.

3.6 Use of personal mobile devices (including phones and tablets)

The Robert Holme Academy allows staff to use their personal device in designated areas around the school (e.g. staff room). Staff should never be seen with their personal device in front of a student, even if it is only to check the time.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child.

Students may bring their own personal device into school, however, it will be handed in upon arrival and stored in a safe, locked place until the end of the day. Under no circumstances should students have their personal devices on them during the day. Students should also refrain from taking and posting images of other students online and on their social medias.

The school is not responsible for the loss, damage or theft of any personal mobile device that is brought into school and users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Students are not permitted to wear a smart watch (e.g. iWatch or similar), but a fitness tracker (e.g. Fitbit) will be permitted within the school.

3.7 New Technological Devices

As stated in the introduction, we now live in a world that has amazing and exciting new technologies provided to us year after year. With this in mind, new personal technological devices may offer opportunities for teaching and learning. However, the school must consider whether they offer any additional educational benefit and carry out risk assessment before use in school is allowed. Parents/carers, pupils and staff should not assume that new technological devices will be allowed in school and should check with the Headteacher or Managing Director before they are brought into school.

3.8 Reporting incidents, abuse and inappropriate material

The Robert Holme Academy recognises that there may be occasions in school where either a student or staff receives offensive, abusive or inappropriate messages. Students and staff may also find themselves, by accident, accessing upsetting or abusive material.

If this happens the student or member of staff should:

- Report it immediately to the first member of staff available (students);
- Report it to the online safeguarding lead, the Designated Safeguarding Lead and/or the Headteacher;
- Undertake an initial assessment and decide whether the incident has, or may, lead to significant harm. If this is the case, safeguarding procedures should be followed;
- Report to the police or social care if necessary and a serious incident;
- Report on MyConcern if they are made aware of any instances of abuse, inappropriate usage or cyber-bullying.

3.9 Curriculum

The Robert Holme Academy is aware that the students in our care may face additional challenges to those of their peers due to their additional needs. The Robert Holme Academy has developed a curriculum that fully embeds online safety and we have an ethos of being a 'Telling School' so that students and staff can discuss any concerns openly with us.

Our curriculum allows students to become informed, safe and responsible online, recognising that their digital footstep may lead to repercussions in the future, and how to protect themselves from this online. In order to do this, we have a dedicated PSHE curriculum, circle time, assemblies, personal development lessons and an SMSC Calendar.

Our curriculum is flexible and adaptable and can be used to respond to any immediate online safety issues and risk.

The Robert Holme Academy are also dedicated to explicitly teaching about the dangers of radicalisation in all form in order to support the counter extremism and terrorism drive.

Our curriculum is designed to support students in understanding how to use the internet, mobile and digital technologies safely and responsibly. However, the The Robert Holme Academy recognises that our students may face additional challenges online due to the special needs of our students. Due to this, our curriculum aims to include areas such as:

- understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity;
- learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment;

- developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
- thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others;
- understanding the permanency of all online postings and conversations Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images;
- understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help;
- how the law can help protect against online risks and abuse.

Students are not asked to use their online presence within school to communicate with others, either internally or externally. If this was planned as part of a learning opportunity, further permission would be sought from parents/carers.

3.10 Staff Training

The Robert Holme Academy is dedicated to training our staff to fulfil their roles in online safety as effectively as possible.

We regularly audit the training needs of our school/staff by monitoring the current trends of issues and risks that may be posed to our students and staff using internet, mobile and digital technologies.

Upon induction, staff are provided with a copy of this policy and an Acceptable Use Agreement. Staff must read the policy and sign the agreement before having contact with the students.

3.11 Working in partnership with parents/carers.

The Robert Holme Academy is committed to providing and guiding parents/carers to online safety information in order to help keep their child as safe as possible online. However, it is important to note that parents/carers must understand that they play a key and crucial role in supporting their child to behave and conduct themselves appropriately online, and to explain that actions online can have serious repercussions both now and in the future.

The school provides regular and updated online safety information via the school's website, social media profile and communications with home. From time to time, the school will also provide face to face training/discussions with parents in order to empower them in having a greater understanding of the internet, mobile and digital technologies used in today's society, with the aim to enable them to support their child to be safer and more responsible online.

Annually, parents/carers are asked to read, discuss and co-sign the Acceptable Use Agreement with their child so that they are aware of the school's expectations and the student and parent/carer responsibilities.

3.12 Records, monitoring and review

All breaches of this policy must be reported and logged on the appropriate form. All staff have a professional responsibility to record breaches and incidents correctly and report them on MyConcern.

The Robert Holme Academy supports students and staff who have been affected by a breach in this policy. If inappropriate or illegal use of internet, mobile and digital technologies has been found to have happened, the school reserves the right to implement the behaviour policy for students and disciplinary policy for staff. In some circumstances police and social care may be contacted depending on the breach.

The Managing Director will review the data records of breaches on a termly basis and hold those to account who are responsible for implementing the policy.

Appendix 1

Acceptable Use Agreement - Students

Student: please read the following agreement and discuss it with your parents/carers and class teacher.

Parents/carers: please read and discuss this agreement with your child and then sign it, ask your child to sign it, and return it to the school.

If you have any questions or concerns, please speak to Peter Lawrence (Online Safety Lead).

Student agreement:

- I will be responsible for my behaviour when using the internet, including social media platforms, games and apps. This includes the resources I access and the language I use.
- I will not deliberately browse, download or upload material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to a member of staff.
- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not give out any personal information online, such as my name, phone number or address.
- I will not reveal my passwords to anyone.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- If I am concerned or upset about anything I see on the internet or any messages that I receive, I know I will tell a member of staff.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.

I understand that my internet use at Robert Holme Academy will be monitored and logged and can be made available to the group leader. I understand that these rules are designed to keep me safe and that if I choose not to follow them, Robert Holme Academy may contact my parents/carers.

Signatures:

We have discussed this online safety agreement and [insert child's name] agrees to follow the rules set out above.

Parent/carer signature…….. Date ……

Student signature…….. Date ……

Appendix 2

Acceptable Use Agreement - Staff

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors are aware of their responsibilities in relation to their use. All staff , including volunteer and agency/supply staff are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with the Headteacher/DSL/Online Safety Lead. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Headteacher/Managing Director/DSL/Online Safety Lead

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, Headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

Social networking

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become ‘friends’ with parents/carers or students on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils. This includes ex-pupils who are also known to be ‘vulnerable’ young people up to the age of 25.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, directors, parents/carers or students. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in Confidentiality and Data Protection policy. Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely and personal data can only be taken out of school or accessed remotely when authorised by the Headteacher.

Images and videos

I will only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

Use of email

I will use my school email address for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses for personal matters or non-school business.

Use of personal devices

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will only use approved personal devices in designated areas and never in front of pupils.

I will not access secure school information from personal devices without the Headteacher's permission.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of the Headteacher and/or Managing Director.

Promoting online safety

I understand that online safety is the responsibility of all staff and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, visitors, students or parents/carers) to the DSL/Headteacher/Managing Director (online safety lead).

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with a member of SLT.

Video conferencing

I will only use the conferencing tools that have been identified and risk assessed by the Managing Director. A school-owned device should be used when running video-conferences, where possible.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment.

Signature …… Date ……

Full Name …….. (printed)

Job title ……