Riviera Education Trust

'Inspiring the individuals of today, for a better society tomorrow,

"Aspire, Belong, Collaborate"

ONLINE SAFETY POLICY

Review Frequency	Annual
Reviewed	19/12/25
Next Review	December 2026
Agreed by Trustees	19th December 2025

Oldway Primary School

ROSELANDS PRIMARY SCHOOL

SHIPHAY LEARNING ACADEMY

Contents

Rationale

Digital technologies have become integral to the lives of children and young people in today's society, and for the 21st century, both within schools and in their lives outside school.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. Unfortunately, the use of these new technologies can place young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images, video games or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact with on the internet
- The sharing and distribution of personal images without an individual's consent or knowledge
- Inappropriate communication and contact with others, including strangers
- Sexting
- Implications of Geolocation
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the "offline world" and it is essential that this online safety policy is used in conjunction with other school policies (e.g. anti-bullying, child protection and GDPR policies).

Development, Monitoring and Review of this Policy

This online safety policy has been developed by the: Online Safety Team (IT Subject Leader/Online Safety Lead/DSL/Technologies Manager) in collaboration with parents, pupils and governors.

Consultation with the school community has taken place through staff meetings, School Council, parents via school website / newsletters/ Pastoral Committee of the governing body and the Computing Subject Leaders.

It is to be reviewed at least every year by the IT Subject Leader, Designated Safeguarding Lead, Pastoral Team Manager and Online Safety Governor. Riviera Education Trust recognises the need for

this policy to be reviewed more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place.

The implementation of the policy will be monitored by the IT Subject Leader, IT Team and Designated Safeguarding Lead.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Senso alerts to DSLs and Head of School
- SWGfL monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of students, parents and carers

Policy Statements

- Teachers will plan Online safety lessons as part of Computing, PHSE and other lessons and lessons will be regularly revisited – this will cover both the use of IT and new technologies in school and outside school
- Key online safety messages should be reinforced as part of a planned programme of assemblies and regular lessons, including during anti-bullying week and Safer Internet Day.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information, at both at home and in school.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school IT systems, both in and out of school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate online safety behaviour that take place out of school.

- Please refer to Acceptable Use Policy for each school

ROLES & RESPONSIBILITIES

The **Head of School** is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead, the IT Subject Leader/Online Safety Lead and the Technologies Manager.

Any online safety issues must be reported to the Designated Safeguarding Lead and appropriate action should be taken, this should be logged by the Technologies Manager into the online safety log with the following information:

The **Technologies Manager and IT Subject Lead** are responsible for ensuring:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

Date	Incident (including details, who it concerns, IP address if available)	Logged by	Actions

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices. The IT Co–Ordinator/Online Safety Lead will attend online safety training and use staff meetings to pass on this information.

- they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Designated Safeguarding Lead, IT Subject Lead and Technical Manager
- digital communications with pupils (email/blog/Google Drive/Zoom) should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school online safety and *Pupil Rules for Responsible Computer Use*
- deliver regular online safety lessons
- monitor IT activity in lessons, extra-curricular and extended school activities
- Be aware of online safety issues related to the use of mobile phones, cameras and hand held devices like iPads and that they monitor their use and implement current school policies with regard to these devices

The principles of positive relationships also apply online especially as, by the end of primary school, many children will already be using the internet. When teaching relationships content, teachers should address online safety and appropriate behaviour in a way that is relevant to pupils' lives. Teachers should include content on how information and data is shared and used in all contexts, including online; for example, sharing pictures, understanding that many websites are businesses and how sites may use information provided by users in ways they might not expect. Reference DfE

statutory guidance Relationships Education, Relationships and Sex Education (RSE) and Health Education, page 19, paragraph 58 of the document:
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090195/Relationships_Education_RSE_and_Health_Education.pdf

In addition to this staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT. The Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, the Trust will treat this as a data breach, and will follow the personal data breach procedures.

Pupils

- are responsible for using the school IT systems, at home and school in accordance with the *Pupil Rules for Responsible Computer Use*, which they will be expected to understand and sign before being given access to school systems. See further section on curriculum/pupil use.

Parents and Carers

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and the school website and Twitter feeds.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take and use digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- In addition to this all parents of children in the school must sign to agree that their children either may or may not be photographed and appear on the school website or in local newspapers.

Use of mobile telephones

- Pupils may bring mobile telephones to school but should leave them at the office for the duration of the day.
- Staff may bring mobile telephones to school but must use them in the staff room during the school hours and not in class other than for the use of 2 Factor Authentication for school accounts.

Communications

- The official school email service may be regarded as safe and secure and is monitored.
- Users must immediately report to the Technologies Manager – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and pupils or parents and carers must be professional in tone and content.
- Staff should not communicate with children out of the school environment, unless it is on an approved private domain that has been authorised by the IT Coordinator and Head of School (e.g. Google Drive/Google Classroom).
- Staff may use social networking sites at their own risk and should ensure that security settings are high and that professionalism is kept.

Curriculum/Pupil Internet Use

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in the safe and responsible use when online is therefore an essential part of the school's online safety provision.
- A planned online safety programme will be provided as part of IT/ PSHCE /other lessons and will be regularly revisited by the pupils to learn the risks of e-communication (personal details, viruses, phishing, cyber-bullying, Internet risks, copyright, longevity of posted information/images, social media use, etc.)
- Key online safety messages are reinforced in assemblies.
- Rules for use of IT systems / internet are posted in rooms and displayed on computer screens.
- Pupils may only use computers/digital resources under the supervision of a member of staff – the adult may not necessarily be standing over them and the pupils have responsibility for following the responsible technology use rules at all times.

- Pupils may only use the Internet to search for resources to use for curriculum learning unless specifically given permission otherwise.
- The use of websites for other purposes i.e. to play games, is only permitted by prior agreement with a member of staff. Lunch Club, Breakfast and Late Clubs may only access approved sites.
- Parents will be informed about pupils playing inappropriate games outside of school.
- Pupils must ask for permission before searching using Google Images.
- Pupils not using computers responsibly will be denied freedom of access and their parents will be informed.
- Pupils must be advised as to the social, health and emotional impact of the excessive use of e-technologies.
- The school has the right to confiscate electronic devices, and to search for and delete information from them, as per the school Behaviour Policy.

Images

- Pupils must obtain the permission of the subjects for all digital images and agree the purpose of their use, before using them as per the GDPR policies. Photos covered by the Digital Image Consent Form may be kept by the school for its archives.
- Publication of video/still images is subject to the approval of the participants and where appropriate, parents/guardians.
- Images of pupils/use of names may not be published for access externally without the permission of the Head of school/ Deputy Head, unless covered by the Digital Image Consent Form.
- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing images on the internet e.g on social networking sites.

Information

- Pupils may only take digital information from school (via USB or Google Drive) with the permission of a member of staff. The information should be focused on learning.
- During IT lessons, pupils will be made critically aware of plagiarism, quality, accuracy, bias and relevance of information. This work will be followed up when cross-curricular opportunities arise.

Communication

- Some pupils may currently communicate beyond school via school systems such as Google Classroom which must be monitored by the class teacher.
- Pupils should be taught about email, messaging and video conferencing safety issues, such as the risks attached to the use of personal details and conversing with strangers. They should also

be taught strategies to deal with inappropriate contact/content and be reminded of the need to communicate clearly and correctly and not include any unsuitable or abusive material.

- Users must immediately report the receipt of any email or message that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, google drive, etc) must only take place on official (monitored) school systems.
- All incidents must be reported by the pupil to the class teacher, who can inform the Technical Manager/Online Safety Lead/Safeguarding Lead/ Head of School if appropriate.

Incident Monitoring and Review

- Incidents must be logged on school safeguarding reporting systems (e.g. CPOMS, Senso) and communicated to the Safeguarding Lead.
- Staff will be kept up to date with developments via staff meetings/training.

Appendix 1 – STAFF/ VOLUNTEER Acceptable Use Policy

School Policy

This Acceptable Use Policy reflects the RET school online safety policy. The school will ensure that staff and volunteers will have good access to IT to enable efficient and effective working, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) applies to staff, volunteers and guests who have access to and are users of school IT systems and to school related use of IT systems outside of school.

My Responsibilities

I agree to:

- read, understand and act in accordance with the School Online Safety policy
- report any suspected misuse or concerns about online safety to the Designated Safeguarding Lead
- monitor IT activity in lessons, extracurricular and extended school activities
- model the safe use of IT
- refrain from publishing any information that: may be offensive to colleagues, may breach the integrity of the ethos of the school or may bring the school into disrepute (this includes personal sites)

Education

- I understand that I am responsible for the online safety education of pupils
- I will respect copyright and educate the pupils to respect it as well

Training

- I understand that I will be required to participate in online safety training
- I understand that it is my responsibility to request training if I identify gaps in my abilities

Cyberbullying

- I understand that the school has a zero tolerance of bullying. In this context cyberbullying is seen as a type of bullying.
- I understand that I should report any incidents of bullying in accordance with school procedures

Technical Infrastructure

I will not try to by-pass any of the technical security measures that have been put in place by the school. These measures include:

- the proxy or firewall settings of the school network (unless I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)
- **Passwords**
    - I will only use the password(s) given to me

- I will never log another user onto the system using my login
- **Filtering**
  - I will not try to by-pass the filtering system used by the school
  - If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised (i.e. YouTube)
  - I will report any filtering issues immediately
- I understand that the school will monitor my use of computers and the internet

Data Protection

- I understand my responsibilities towards GDPR and will ensure the safe keeping of personal data at all times.
- I will ensure that all data held in personal folders is regularly backed up

Use of digital images

I will follow the school's policy on using digital images making sure that:

- only those pupils whose parental permission has been given are published
- I will not use full names to identify people
- I will ensure when uploading videos to the school's YouTube channel that I have the Head of School's permission and only use the school's own channel for this purpose.

Communication

I will be professional in all my communications and actions when using school IT systems.

Email

- I will use the school provided email for all business matters
- I will not open any attachments to emails, unless the source is known and trusted (due to the risk of the attachment containing viruses or other harmful programmes).

Social Media

- I will ask permission before I use social media with pupils or for other school related work.

Personal publishing

- I will follow the Online Safety policy concerning the personal use of social media

Mobile Phones

- I will not use my personal mobile phone during contact time with pupils without permission from the School Leadership Team.
- I will not use my personal mobile phone to contact pupils or parents without permission

Reporting incidents

- I will report any incidents to either the Online Safety Lead/Technologies Manager
- I will make a note of any incidents in accordance with school procedures
- I understand that in some cases the Police may need to be informed

Sanctions and Disciplinary procedures

- I understand that there are regulations in place when pupils use IT and that there are sanctions if they do not follow the rules.
- I understand that if I misuse the school IT systems in any way then there are disciplinary procedures that will be followed by the school.

I have read and understand the full Online Safety policy and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) in a responsible and professional manner as outlined in that document.

Staff/Volunteer Name _____

Signed _____

Date _____

Appendix 2 – TECHNOLOGIES MANAGER Acceptable Use Policy Extension

The school Technologies Manager (or person given similar responsibilities) is placed in an exceptional position of trust. Many of the duties that the Head of school expects the Technologies Manager to complete are included in the Staff Acceptable User Policy of the school.

This document is not a job description but an addition to the Staff Acceptable User Policy that allows the Technologies Manager to fulfil these duties.

Areas of concern are that:

- Files may be created, imported or processed by staff and pupils and stored on the school's servers, Google drive or other storage systems (e.g. USB memory sticks, SD cards etc.) that might be of an inappropriate nature to the school setting. Inappropriate use includes any production, processing or transmission of offensive, provocative, racist, unethical, irreligious or anti-social materials in any format. Also included in this area are any materials that are against the rules and conditions of service for the school e.g. material that might bring the establishment into disrepute. Work created during the school's time or on the school's equipment or on one's own equipment but for school work, belongs to the school.

- User accounts will need to be created and serviced meaning that there may be access to these accounts by the Technologies Manager.

- Through work within the school's administration network the Technologies Manager may be placed in the position of assisting in the processing of confidential information including children's health or MIS data, confidential letters or information from or to senior staff, budgeting plans etc.

- The Technologies Managers through specific user names and password have control, (sometimes through remote workstations) to the school's network

Because of the importance of these areas of data management the Technologies Manager should:

- be responsible for monitoring the school's network.

- be given permission to access other user's files.

- protect the users by maintaining a filter for the school.
- monitor the internet use of users within the school.

- be aware of the laws relating to the use of computers especially those around Data Protection, Copyright and those referred to in the school's Online Safety Policy and AUPs.

- make sure that they record all user names and passwords for all the services they access in a place where the senior leaders in the school can access them.

- have their use of the school's network, internet and other aspects of their work open for scrutiny.

To enable them to discharge these duties they should:

- receive training on the sensitive nature of their job especially in relation to GDPR and the confidentiality of information.
- have an agreed procedure for managing the internet filter. This should include a log of decisions made.
- have an agreed understanding of what is expected of them as far as the regular monitoring of the network system and internet.
- have agreed procedures for reporting incidents.
- log any incidents including minor ones that are quickly resolved.
- be careful to make sure that they are observed when investigating serious incidents to make sure that they are protected against any allegations that could arise (e.g. never open websites that are suspected of having inappropriate material unless others are present).
- have frequent meetings with their line manager to report on any issues or trends.

As a Technologies Manager (or a person who has similar responsibilities) I have read the above document and understand that I will be directed by senior staff to complete work outside of the Staff Acceptable User Policy.

I will report all concerns I have to the appropriate member of Senior Management.

Name: _____

Signed: _____

Senior Member of Staff: _____

Date: _____

Appendix 3 – VISITOR Acceptable Use Policy

Visitors should apply certain standards when using computer equipment in schools.

These standards should include an awareness of GDPR and Copyright laws.

Logging in

- If you use the school's equipment, then request a guest log in.
- If you are using equipment that has been logged in by a member of staff, always ensure a member of staff is present. Always lock the machine if you need to leave the room.
- If your service contract (Network/MIS support) allows you access to the system through team logins inform the school how you will be accessing the system.

Wireless Access

- Request permission to use the wireless connection (if available) asking for an authorisation key. You may need to change proxy settings.
- Remember that bandwidth is limited so avoid intensive use such as large downloads.

Internet Access and uploading

- The schools Internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the schools normal filtering system. This might not be possible as changes to the filter can take some time.
- You are responsible for the sites that appear on any machine that you are using. Report any issues with the member of staff present.
- Never upload and install software or updates without permission from a member of staff.

If you use your own equipment:

- Make sure that it has up to date virus protection software installed.
- That you take care with trailing wires.
- That you can identify your equipment.
- Never leave your equipment unattended or in an unlocked room.

Downloading files or documents

For all files

- Make sure that the USB stick/external hard drive has recently been virus checked.
- Never transfer files unless you have permission.
- Make sure that you clearly state the purpose for transferring these files.
- Check to see if the school machine you would like to transfer files from or to is encrypted as it might automatically encrypt your USB stick/hard disc drive.

If the file contains sensitive personal data such as staff or student information

- Get permission for this in writing or by email.
- (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed).

- Use an encrypted memory stick or hard drive.
- Transfer the file only over a secure email connection.

If you take pictures, video or sound files then check

- That you have permission to capture these files.
- That the staff/children have all given their permission for these images/voices to be used.
- That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

Name: _____

Signed: _____

Date: _____

Appendix 4 – BRING YOUR OWN TECHNOLOGY (BYOT) Acceptable Use Policy

As new technologies continue to change the world, they also provide many new and positive educational benefits for teaching and learning. To encourage this growth, we are allowing students to bring their own technology into school and use them in lessons.

This Acceptable User Policy helps educate and inform pupils about the use of their technology on the school site.

Definition of technology
For purposes of BYOT, technology means any privately owned portable equipment such as laptops, games devices, smart phones, cameras, any device capable of accessing the internet etc.

Internet
Only the internet connection provided by the school may be accessed while on the school site. Accessing the internet through a signal that does not go through the filtered access provided by the school is not allowed at any time.

Security and Damages
Responsibility to keep the device secure rests with the individual owner. The school, nor its staff or employees, are liable for any device stolen or damaged on the school site. If a device is stolen or damaged, it will be handled through the school policies similar to other personal belongings. It is recommended that decals, other custom touches and UV markings are used to physically identify the device. Protective cases should be used as well. If the device is capable of being GPS tracked then this should also be activated.

BYOT Pupils Agreement
The use of technology to provide educational material is not a necessity but a privilege. A pupil does not have the right to use his or her laptop, mobile phone or other electronic device while at the school. When abused, privileges will be taken away.

Pupils and parents or guardians partaking in BYOT must adhere to the pupil code of conduct, as well as all other school policies, particularly the e-safety policy and the associated Responsible PC Use.

Additionally, technology:

- Must be in silent mode on the school site and on school buses
- May not be used in tests
- Must only be used to access files or computer or internet sites which are relevant to the curriculum. Games are not permitted

Pupils acknowledge that:

- The schools network filters will be applied to the internet connection and attempts will not be made to bypass them
- Their personal device is virus protected and is not capable of passing on infections to the schools network

- Hacking, damaging or bypassing the school internet security procedures is against the school policies
- The school has the right to collect and examine any device that is suspected of causing problems, either technical or from abuse of other school policies
- Printing from personal devices will not be possible
- Personal technology is charged prior to bringing it to school and runs off its own battery. Charging will not be possible during the school day

Bring Your Own Technology (BYOT) Agreement

Please read and sign the BYOT agreement. No pupil will be allowed personal technology devices unless the agreement is signed and returned.

Pupils, parents and guardians participating in BYOT, must adhere to all school policies.

Please read carefully and initial every statement

_____ Pupils take full responsibility for their devices. The school is not responsible for the security of personal technology. Personal devices cannot be left on school property before or after school hours

_____ Devices cannot be used during tests

_____ Pupils must immediately comply with the teachers request to shut down or close devices. Devices must be in silent mode and put away when asked by teachers

_____ Personal devices must be charged prior to bringing them to school and run off their own batteries while at school

_____ To ensure appropriate network filters, pupils will only use the school internet connection and will not attempt to by-pass this

_____ Pupils must make sure that their device is virus protected and is not capable of infecting the school network

_____ Pupils realise that printing for personal devices will not be possible

_____ Pupils should not share their device with other students, unless they have written permission to do so

_____ The school retain the right to confiscate and examine any device

_____ The school will inform parents or guardians of any misuse and in some cases, if confiscated, only return the device to the parent or guardian

Please understand that the use of personal devices to support educational experience is not a necessity but a privilege. With respect of the rules, this privilege will benefit the learning environment as a whole. When rules are abused, privileges will be taken away.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my technological privileges as well as other disciplinary action.

Pupil Name _____

Pupil Signature _____

Date _____

Parent/Carers name and signature _____

PUPIL RULES FOR RESPONSIBLE COMPUTER USE

The school's computers are provided to help our learning. The following rules will allow us to use them fairly and safely.

- I will only access the system with my login and password.
- I will not access other people's files without their permission.
- **I will only use the computers/devices for schoolwork, unless I am given permission.**
- I will not bring in USB memory sticks from home without permission.
- I will not take or use images/video of other people without their permission.

THE INTERNET

- I will only use the internet **after first asking a member of staff.**
- I will only use e-mail when told to by a teacher, and will not e-mail anyone I don't know. All messages I send will be polite and responsible.
- I will report anything that I think could be cyber-bullying.
- I will only use Google images, listen to music or watch videos after getting permission from an adult, including on my own personal devices.
- I will tell an adult if I see anything that I think is offensive, or may harm a computer (i.e. viruses), whether it happens when I use a computer, or when someone else does.
- I will not download or install files from the internet.

- I won't try to access sites which are not suitable for use in school.

Signed _____

DETAILS OF AMENDMENTS

September 2019

- Updated to cover general expectations and use for all RET schools.

June 2020

- Added, Head permission required to upload digital images to School YouTube channel.

August 2021

- Reviewed 22.7.21 (J Christian) NB Remote Learning Policy should sit alongside this policy.

July 2023

- Reviewed 13.7.23 without change.

18 April 2024

- Addition of Artificial Intelligence (AI) restricted use.

10 October 2024

- Added, Senso alerts
- Pupil mobile phones also to be handed to teacher to be safely stored
- Grammatical changes – ICT changed to IT
- Reporting to DSL in line with updated DfE Keeping Children Safe in Education statutory requirement

4 November 2025

- Under use of mobile phones, added 2 Factor Authentication as a reason for staff to use their phones.

December 2025

- Appendix 2 Pupil/Parent Acceptable Use Policy removed
- References to the above document replaced with a reference to the *Pupil Rules for Responsible Computer Use* document (Appendix 5)