Winchelsea School

Winchelsea School

Guernsey Road
Poole BH12 4LL

Online Safety Policy – (Previously E-Safety)			
Version	**3**	**Review Date**	**February 2026**
Review Cycle	**Annually**	**New Review Due**	**February 2027**
Author / Owner	**Alex Dunnachie**		

WINCHELSEA SCHOOL ONLINE SAFETY POLICY

Introduction

In the community of Winchelsea everyone is important. Winchelsea is a place where everyone feels welcome, has a voice, is safe, able to achieve and have fun.

This policy is based on advice from the Department for Education (DfE) guidance on:

- Keeping Children Safe in Education;
- Teaching online safety in schools;
- Preventing and tackling bullying;
- Cyber-bullying: advice for headteachers and school staff;
- Relationships and sex education;
- Searching, screening and confiscation.

It also refers to the DfE'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 cyber-bullying 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.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Identify and support groups of pupils that are potentially at greater risk of harm online than others;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 Key Categories of Risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization, misinformation, disinformation, and conspiracy theories and extremism;
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and;
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

Roles and Responsibilities

Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). The Governor with delegated responsibility for online safety is also the Safeguarding Governor.

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);
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable pupils, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

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

The Designated Safeguarding Lead

Details of the school's DSL and his team are set out in the Safeguarding Policy as well as relevant job descriptions.

The DSL takes 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 and Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;
- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks;
- Working with the Network Manager to make sure the appropriate systems and processes are in place;
- Managing all online safety issues and incidents in line with the school Safeguarding Policy;
- Ensuring that any incidents of cyber-bullying are logged and managed appropriately in line with the school Behaviour Policy;
- Ensuring that any online safety incidents are logged through the schools safeguarding and reporting system, Child Protection Online Management System (CPOMS) are 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;
- Liaising with other agencies and/or external services if necessary;
- Providing regular safeguarding updates to all staff and work with the Online Safety Champion to ensure online safety training is delivered annually in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

The Online Safety Champion

The Online Safety Champion takes lead responsibility for online safety in school, in particular:

- Updating and monitoring on the Online Safety Curriculum;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated annually to assess effectiveness and ensure pupils are kept 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;
- The school has various online filtering systems across it's sites. Inappropriate content and searches are blocked. The Network Manager reserves the right to search for specific conflicts when requested.

Site	Filtering Provider
Winchelsea	Netsweeper
Canford	NetSweeper
Magna	Netsweeper
Oldtown	Netsweeper(Externally Managed)
Kinson	SchoolProtect(Externally Managed)
Post16	Sophos Cloud Filter
Broadstone	SWGFL

- The School has a flagging system Smoothwall Monitor that will alert the Network Manager of inappropriate searches and keystrokes;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Maintaining a log of unblocked online sites and the reasons why they are unblocked;
- Ensuring that any online safety incidents are shared with the DSL;

This list is not intended to be exhaustive.

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)
- The DSL to ensure that all new starters to Winchelsea School receive training and a login to report any online safety incidents through Winchelsea School's online safeguarding reporting tool, CPOMS;
- Working with the DSL to ensure that any online safety incidents are logged through CPOMS 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;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here';
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting both the DSL and Network Manager ;
- Following the correct procedures by contacting the Network Manager if they need to bypass the filtering and monitoring systems for educational purposes;
- Completing training as requested.

This list is not intended to be exhaustive.

Parents / Carers

Parents / Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Ensure their child (as far as is practicable) has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet;
- Parents / Carers can seek further guidance on keeping children safe online from the following organisations and websites:

    - What are the issues? – UK Safer Internet Centre / vodafone.co.uk/mobile/digital-parenting;
    - Hot topics – Childnet International;
    - Parent resource sheet – Childnet International;
    - The National College - The National College | CPD for Schools, Trusts, Colleges & Nurseries

Pupils

Pupils will use different a range of different technologies which may or may not have access to the internet. Different pupil groups will be expected to take on different responsibilities' dependent on their curriculum pathway.

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 relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the Winchelsea ICT Curriculum alongside RSE taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

Educating Parents / Carers about Online Safety

The school will raise parents/carers' awareness of online safety by directing them to online resources and through the subscription to the National Online College. The National College provides a range of up-to-date courses, guides, explainer videos and resources to support their understanding of online safety.

In addition, Winchelsea School will raise parents' awareness of internet safety through the school termly newsletter and other communications home, and in information via our website.
This policy will also be shared with parents/carers.

Opportunities to discuss online safety will also be provided during parents' evenings. The school will let parents/carers know:

- What systems the school uses to filter and monitor online use;
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher and then DSL or Online Safety Champion. Concerns or queries about this policy can be raised with the Headteacher or DSL.

Summary of Meeting Statutory Guidance

An outline of Winchelsea's Online Safety Curriculum in relation to statutory guidance and safeguarding procedures:

a) Opportunities to embed **cross curriculum learning** and debate with PSHE with in proposed drop days.
b) Understanding and supporting **Content**, **Conduct**, **Contact & Commerce**
c) Curriculum and Spiritual, Moral, Social and Cultural **(SMSC)** development links to support the embedding of Online Safety concepts
d) **Trusted resources and supporting partners** to go to for additional resources guidance and support.
e) **Pupil voice** in Online Safety related issues through the Pupil Passport.
f) Reporting of incidents of concern raised in lessons and the **safeguarding procedures.**

Winchelsea recognises internet safety has strong cross curricular links to PSHE. Elements of online behaviour, relationships and consent are woven into the PSHE and Relationships and Sex Education (RSE) curriculum by the PSHE lead (Lee Riviello).

Online Safety Curriculum

The Winchelsea Online Safety curriculum aims to provide children with the skills and knowledge to become active citizens and interact safely online in the digital world. We recognise the additional vulnerabilities of the pupils at Winchelsea school linked to their SEND. These include access to, or the intentional or unintentional production of, inappropriate **content** which can be scary, misleading or developmentally scaring. Misunderstanding of appropriate online **conduct** and behaviour placing them at risk to a variety of forms of exploitation. This can potentially lead to undesirable **contact** from those wishing to exploit their vulnerabilities. Additional risks to pupils in understanding risks such as online gambling, inappropriate advertising, phishing and/or financial scam **commerce**.

It is important to dispel the myth that online and offline lives are different but in fact intertwine as one and the same thing where behaviours online and offline should mirror each other. To support the consolidation, Online Safety is not solely found in discrete lessons but has cross curricular links predominantly with **PSHE** and can also be found within **SMSC** links.

The online safety framework used at Winchelsea School is From the National College and focusses predominantly on eight different aspects of online education.

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

Teachers conduct a baseline assessment for all pupils to determine at which stage they access this framework and the related planning and resources. If pupils are not at the base level for accessing the online safety curriculum, then they will continue to develop their core skills through ICT lessons and other cross-curricular areas.

Winchelsea School will raise parents' awareness of internet safety through the school termly contact service Arbor and other communications home, and in information via our website.

Parents can also request a login to access Online Safety Guides & Resources for Parents (nationalcollege.com). This provides a range of up to date courses, guides, explainer videos and resources to support their understanding of online safety.

This policy will also be shared with parents on the school website containing:

- Links for support and reporting of internet safety concerns;
- User guide to support social media use;
- Links to the latest apps, movies and games through 'net aware' and 'common sense media'

- Addition internet safety advice from SWGfL (South West Grid for Learning).

Online safety will also be covered during parents' evenings.

During online safety week https://www.saferinternetday.org/ additional resources are sent home through the School contact service Arbor

Cyber-bullying

Definition

Cyber-bullying 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 or Anti-Bullying Policy.)

Preventing and Addressing Cyber-bullying

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.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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 report the incident and provide the relevant material to the Police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.
We recognise that in most instances of perception of bullying may in fact be peer conflict. School leaders will always aim to support pupils the impact of their actions and how to manage online interactions more appropriate. Leaders will also encourage parents / carers to be actively engaged in the online behaviour of their child.

To help prevent cyber-bullying, we will support pupils to 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. The Enquirers pathway of school will discuss cyber-bullying with their classes when there are at the level they can understand the concept, beginning with Conduct in Online safety unit 1 of the curriculum.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

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.

How the School will Respond to Issues of Misuse

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 / staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Examining Electronic Devices

The Headteacher, and other members of the Senior Leadership Team can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or;
- Is identified in the school rules as a banned item for which a search can be carried out, and/or;

- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from [the headteacher / DSL);
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- Seek the pupil's co-operation;
- Please see the Behaviour Policy for how pupil searches should be managed.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or;
- Undermine the safe environment of the school or disrupt teaching, and/or;
- Commit an offence.

If inappropriate material is found on the device, the Senior Leader will decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, the Senior Leader must consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the Police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, the Senior Leader may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or;
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image;
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- The Winchelsea School Behaviour Policy.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Winchelsea School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Winchelsea School will treat any use of AI to bully pupils in line with our Anti-bullying / Behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

See our AI Policy for further information

Acceptable Use of the Internet in School

All pupils, parents / carers, 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 & 2) which are collated by the administration team and stored in reception in each pupil's individual file.

Staff forms are collated and retained by the Administration Manager.

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 to ensure they comply with the above.

More information is set out in the acceptable use agreement in Appendix 1 and 2.

Pupils using Mobile Devices in School

Pupils may bring mobile devices into school but are not permitted to use them during the school day. Pupils are expected to hand in their mobile devices at the start of the school day, devices will be given back to pupils at the end of the school day. If a pupil does not surrender their mobile device this may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Data will not be taken off the school site with an unencrypted data stick;
- Documentation can be accessed from home with the use of Microsoft OneDrive, schools secure emails or by sing remote access installed by the ICT support team;
- Making sure the device, including school desktops computers around school, are locks if left inactive for a period of time (Windows key + L);
- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

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 our school's Behaviour Policy and Acceptable Use Agreement. 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 Code of Conduct and the Low Level Policy Reporting all concerns to the Headteacher. Should the concern relate to the Headteacher this must be reported to the Chair of Governors.

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.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Pupils can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages;
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
    - Sharing of abusive images and pornography, to those who don't want to receive such content.

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse;
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up;
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term;

The DSL and Online Safety Champion will undertake 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 Safeguarding Policy.

Monitoring Arrangements

Online behaviour related to concerns that have occurred outside of school will be logged onto CPOMS.

Online behaviour that is of concern in school that has triggered a concern will be logged on the child's CPOM file and then more centrally on a document that includes all concerns as well as any challenges to the monitoring and filtering.

Links with Other Policies

The online safety policy is linked to our:

Safeguarding policy
Behaviour policy
Staff Disciplinary procedures
Data Protection policy and privacy notices
Complaints procedure
ICT and Internet acceptable use policy
Winchelsea School Code of Conduct

Appendix 1

Pupil Acceptable Use Policy Agreement V1

Pupils following a Explorers and Discoverers pathway are expected to:

- Ask an adult if I want to use a computer, tablet or other electronic device;
- Only use activities, applications and websites that an adult has asked or allowed me to use;
- Take care of computers, tablets or other electronic devices;
- Ask for help from an adult if I am not sure what to do or if I think I have done something wrong;
- Tell an adult if I see something that upsets me on the screen;
- Know that if I break the rules I might not be allowed to use a computer, tablet or other electronic device.

(Adapted from SWGfL Acceptable Use Agreement Template, 2022)

Additionally, Enquirers and Navigators Pupils are expected to:

For my own personal safety when online, I will:

- Be monitored;
- Keep usernames and passwords safe;
- Be aware of stranger danger and know that others may not always be who they say they are;
- Not share personal information about myself or others;
- Not arrange to meet people I have met online in real life;
- Report anything I experience which is inappropriate or unexpected straight away.

I understand that everyone has equal rights to use technology in school and:

- This is to help me learn;
- I will not download or upload anything unless I have permission from a school adult;
- I will not use this for on-line gaming, gambling shopping, file sharing or sharing videos unless I have permission from a school adult.

I will behave as I expect others to behave toward me:

- I will respect others' work and property;
- I will be polite and kind when I communicate with others;
- I will not take or share photographs or videos of anyone unless I have permission from all people in the photograph or video.

I know that the school has a responsibility to make sure that the technology is safe and working well:

- I will only use my own personal devices, such as a mobile phone, if I have permission from a school adult;
- I will not access or look at anything which is illegal, inappropriate or unexpected;
- I will not use any programmes or software that might help me to access or look at things which would usually be blocked by the school filtering and security systems;
- I will tell a school adult straight away if any technology equipment is broken or not working properly;
- I will not open any links in emails or attachments, unless I know that the person who sent it is a trusted adult, friend or company;
- I will not try to change the settings on any school computer, iPad or electronic device, unless I have permission from a school adult;
- I will not use any social media sites (e.g. TikTok, Snapchat, Instagram) during school time unless I have permission from a school adult.

When using the internet for research or recreation, I know that:

- I will ask for permission to use the original work of others in my own work;
- I will not try to download copies of work that is protected by Copyright, including music and videos;
- Not all of the information on the internet is true and I should know that sometimes the work of others may deliberately try to lie and trick people.

I understand that I am responsible for my actions, both in and out of school:

- I know that the school has the right to take action against pupils if they behave in an inappropriate or unexpected way online, just as they would in real life. This can also include incidents out of school, where other staff or pupils from the school community are involved (e.g. online bullying, use of images of personal information);
- I understand that if I do not follow this guide, I may be subject to disciplinary action, as per the schools Behaviours Policy. This may also include; loss of access to the school network/internet, contact with parents and in the event of illegal activities involvement of the Police.

(Adapted from SWGfL Acceptable Use Agreement Template, 2022)

Pupil Acceptable Use Agreement Form V1

This form relates to the Pupil Acceptable Use Agreement Form; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement.

Pupil Name: (Learner pathway)	
Pupil Signature:	
Date:	
Parent/Carer Countersignature:	I understand the Pupil Acceptable Use Policy Agreement V1 and am signing alongside or in place of my child. I will communicate all the information in the document at a level my child can understand and process.
Parent/Carer Name:	
Parent/Carer Signature:	
Date:	

Appendix 2

Staff, Supply, Governor & Visitor Acceptable Use Policy Agreement V1 (updated Jan 2026)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use;
- That school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk;
- That staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems;
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, Virtual Learning Environment (VLE) etc.) out of school, and to the transfer of personal data (digital or paper based) out of school;
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school;

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher and or DSL.
- I will be professional in my communications and actions when using school systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission;
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions;
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured;
- I will not use social networking sites for personal reasons on school equipment in school in accordance with the school's policies;
- I will not post on social networking sites whilst on school grounds.
- I will not communicate with pupils on social media platforms.
- I will not engage in any on-line activity that my compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses;
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will ensure that my data is regularly backed up, in accordance with relevant school policies;
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is agreed by a member of the Senior Leadership Team or Network Manager
- I will not disable or cause any damage to school equipment, or the equipment belonging to others;

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage;
- I understand that the Data Protection Policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority;
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school;
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors or the Local Authority and in the event of illegal activities the involvement of the Police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff, Supply, Governor & Visitor Name:	
Signed:	
Date:	

Appendix 3:

SMSC Curriculum Links

Spiritual Development	Moral Development

• Develop and reflect upon personal beliefs and values. • Experiencing Awe, wonder and fascination. • Exploring the Values and beliefs of others. • Willingness to reflect on their experiences. • Using imagination and creativity in learning.	• Developing and expressing personal views or values. • Recognising right and wrong and applying it. • Understanding the consequences of actions. • Investigating moral values and ethical issues (understanding others viewpoints). • Recognise legal boundaries and respect the civil and criminal law of England.
Social Development	**Cultural Development**
• Developing personal qualities and using social skills, including those from different backgrounds and ethnicities to their own. • Participating, cooperating in community life and resolving conflicts. • Understanding how communities and societies function to develop mutual respect towards those that are different. • Develop and demonstrate skills and attitudes that will allow them to participate and contribute to life in modern Britain.	• Exploring, understanding and respecting diversity across the school and the wider community. • Participating and responding to cultural activities (Art, Music, Sport.) • Knowledge of the democratic process and its role in shaping our lives and developing modern Britain. • Understanding and appreciating personal influences that shaped their own heritage and that of others. • Exploring, understanding and respecting different faiths and cultural diversity, both locally, nationally and globally.

Appendix 5: Online Safety Resources List including but not exclusive to:

	NSPCC	SWGfL Safe, Secure, Online	CLICK CEOP Internet Safety	ChildLine 0800 1111
saferinternet.org.uk	nspcc.org.uk/keeping-children-safe/onlinOnline Safety/	swgfl.org.uk	ceop.polic.uk/Safety-Centre/	childline.org.uk
Childnet International		PROJECT EVOLVE Tim*proevo8	IWF Internet Watch Foundation	vodafone Digital Parenting
childnet.com	Azoomee - Search it up	projectevolve.co.uk	Internet Watch Foundation https://www.iwf.org.uk/	Vodafone – digital parenting
	360 degree safe	REPORT REMOVE Nude image of you online? We can help take it down.	REPORT HARMFUL CONTENT	
	360safe.org.uk	Report remove – (Childnet)	reportharmfulcontent.com	