Initial Policy date	January 2022	Next scheduled review	February 2025
Governor approved	February 2024	Key person/people	DHT (Inclusion)
Model Policy	The Key Nov 2023	Model localised	
Pupil leadership team review	N/A	Rotherly Day Nursery variations in policy	Yes

Online Safety Policy

The Westgate School recognises the potential that online resources can bring to support pupils in their education and preparedness for life beyond school. We are committed to supporting young people to become discerning and safe users of online resources, including applications available through mobile devices as well as those on the internet and computers.

The online world knows no boundaries and extends beyond a child/young person's (CYP) time in school. They are engaging with the online world at all times of the day and often, without supervision. Working in partnership with parents/carers, the School is committed to providing support and information such that parents/carers can provide the necessary protection for their child when engaging with online platforms.

Through Partners in Learning events and the regular sharing of information to parents/carers and pupils, the school will continue to support parents to educate and protect their children. As part of this commitment, our school has a specified teacher with responsibility for leading this aspect of our provision. This policy sits within the framework of the recent Keeping Children Safe in Education, Safeguarding and Child Protection policies.

The School has a colleague with responsibility as a Designated Teacher for Online Safety. We will work alongside Year Leaders to respond to individual incidents, maintain an up-to-date knowledge of key issues and lead appropriate professional development for colleagues; liaise with outside agencies; lead Partners in Learning events for parents/carers on a regular basis and, provide and deliver curriculum resources and lessons/assemblies to pupils.

1. 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, radicalisation 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 scams.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and 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.

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

3. Roles and responsibilities

3.1 The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all colleagues undergo online safety training as part of child protection and safeguarding training, and ensure colleagues understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all colleagues receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL) and Designated Teacher for Online Safety.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems such as (SENSO) in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT colleagues and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governing body will co-ordinate regular meetings with leaders to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Ruth Luzmore.

The governor who overseas filtering and monitoring is Philip Davies.

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 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, 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 is responsible for ensuring that employees understand this policy, and that it is being implemented consistently throughout the school.

3.2 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as relevant role profiles.

The DSL takes lead responsibility for Keeping Children Safe in our school, and will ensure that the Designated Teacher for Online Safety is supported in these shared aims:

- Supporting the headteacher in ensuring that employees understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, IT Strategic Lead, IT Network Manager and others, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering colleague training on online safety

- Liaising with other agencies and/or external services as necessary
- Monitoring the School's online safety Help Boxes & Call It Out email account.
- Providing regular reports on online safety in school to the Headteacher and/or governing board
- Providing regular and timely information to parents including Partners in Learning events through the year

This list is not intended to be exhaustive.

3.3 The IT Strategic Lead and Network Manager

These colleagues are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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.
- Conducting a full security check and monitoring the school's ICT systems on an agreed basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy, liaising with external agencies as required.
- Maintain an up to date and effective working knowledge of online security and safety, in partnership with the School's IT provider.

3.4 All employees and volunteers

All employees, 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 and ensuring that pupils follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged 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'.

This list is not intended to be exhaustive.

3.5 Parents and carers

Parents and carers are expected to:

- Support the school in upholding this policy and ensuring that their child is not engaged in harmful activity online.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the IT and mobile devices.
- Ensure that they adhere to the School's Social Media and Online Communications Policy

- Ensure that they are aware of the Malicious Communications Act 1998 in their own use of online platforms and communication, including WhatsApp and email.

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody
- NSPCC: https://www.nspcc.org.uk/

3.6 Visitors, volunteers and members of the community

All those who use the school's IT systems are expected to adhere to this policy.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum (National Curriculum computing programmes of study and guidance on relationships education, relationships and sex education (RSE) and health education).

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Primary Phase:

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

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

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

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

Secondary Phase:

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

Additionally:

The safe use of social media and the internet will also be covered in other subjects where relevant and through the School's curriculum for Personal Development.

Teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and pupils with SEND as appropriate.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, in information via our website, in pupils' Handbooks and, through Partners in Learning events. This policy will also be shared with parents when their child joins our school.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's class teacher or tutor. Low level or early concerns should be shared with the Assistant Year Leader. In a case where a child is at risk of harm or there are ongoing concerns, these must be raised with the School's Designated Safeguarding Lead who will liaise with the Designated Teacher for Online Safety to take appropriate action.

The School will make available to parents information about systems the school uses to filter and monitor online use on request.

6. Cyber-bullying

6.1 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's behaviour policy.)

Cyberbullying can take place between any individuals, including between adults.

6.2 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 has systems in place for pupils to report such concerns: there is a help page on the homepage of the School's website for pupils to use if they need help.

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. Tutors/class teachers will discuss cyber-bullying with their tutor groups.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the School's Behaviour Policy and other relevant policies. Where illegal, inappropriate or harmful material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained and expect parents to work in partnership in the event of such incidents.

If the incident falls within the scope of the Malicious Communications Act (1998), the School will report the incident to the police for investigation and further action. The scope of this is included in Appendix 2. This applies to children, young people and adults in our school community – including parents.

The content of this policy supplements that which is included in the School's Safeguarding and Child Protection Policies.

6.3 Examining electronic devices

School employees have the specific power under legislation to search and confiscate mobile devices where they believe there is a 'good reason' to do so. Only the Headteacher and authorised colleagues can search for and confiscate electronic devices. Grounds for searching and confiscation can be found within the Schools Behaviour Policy and in line with DfE guidance - Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)

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 or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Break any of the school rules and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide on a suitable response. If there are

images, data or files on the device that colleagues 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, colleagues will 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, staff members 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 colleague **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 (or equivalent) 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
- Devices will be handed to the police for action and a report made to Children's Services. Senior colleagues (Year Leaders/AYLs) will follow the School's protocol for responding to incidents such as these according to our 'Safeguarding' and 'Behaviour' Policies.

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

- The DfE's latest guidance on searching, screening and confiscation - Searching, screening and confiscation in schools - GOV.UK (www.gov.uk)
- UKCIS guidance on Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
- Our behaviour policy / searches and confiscation policy

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

6.4 Artificial intelligence (AI)

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

The Westgate 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.

The Westgate School will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour polices.

Employees 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 by the school.

7. Acceptable use of the internet in school

All pupils and adults are expected to behave in line with this policy when using the school's ICT systems and the internet. If using IT/Mobile Devices on our school site, all adults and pupils will be

expected to adhere to the School's policy. Key points will be shared with all visitors on arrival, via our Safeguarding Booklet for Visitors.

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 and adults to ensure they comply with the above.

8. Pupils using mobile devices in school

The School recognises that mobile devices are an intrinsic part of life for young people and is committed to supporting them to use them in a safe and discerning way, such that they do not lead to harm (either for the user or others) or, erode the important aspects of personal and social development.

Pupils may bring mobile devices into school, but are not permitted to use them at any time during the school day or on the school site without the express permission of an adult and only for the purposes of supporting learning.

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

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the School's Behaviour Policy, which may result in the confiscation of their device and a removal of permission for the individual to bring their device into school.

Pupils **must not** have their mobile devices in use at break, lunchtimes or outside of lessons. Mobile devices include but are not limited to: mobile phones, iPads/tablets, smart watches. **If a pupil is using their device at these times they can expect that it will be confiscated and parents may be asked to collect the device from school at the end of the school day.** This is non-negotiable and any breach of these expectations will be dealt with under the School's Behaviour Policy and other respective policies.

9. Employees using work devices outside school

All employees 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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Following instructions for use issued by the School's IT Strategic Lead and Network Manager

Employees must not use the device in any way which would violate the school's terms of acceptable use or that compromises Part B of Teachers' Standards or other relevant policies.

Work devices must be used solely for work activities.

In the interests of managing the workload associated with the increased use of mobile devices and electronic communication, all employees (unless in exceptional and unavoidable circumstances) must follow the School's email protocol (Appendix 3).

10. Employees using personal devices outside school

It is important that this section is read in conjunction with the Safe Use of ICT and Other Devices – for School Colleagues Policy, in particular the Practice and Procedures section for Do's and Don'ts guidance.

- Personal devices must not be used to contact parents or pupils
- Under no circumstances must personal devices be used to photograph or record pupils or other employees
- Employees are not expected to use personal devices for means of work-related communication and all team leaders must take account of individual wishes in relation to platforms such as WhatsApp and in all cases, avoid the use of such mediums where they result in increased workload or as a management tool.
- Employees are not expected to contact parents/carers or external agencies outside of School working hours (Monday- Friday, 8.20am to 6pm, term time only) unless the matter relates to safeguarding or child protection.
- Employees and volunteers must be aware of their online presence as they would do so with their conduct in person inside and outside of school to ensure that they do not undermine the expectations set out in Part Two of the Teachers' Standards (DfE, 2021):

  "A teacher is expected to demonstrate consistently high standards of personal and professional conduct" and to ensure that "Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school".

  This expectation applies to all adults working and volunteering in the school.

11. Training

All new employees 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 employees 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, meetings and briefings from the Designated Teacher for Online Safety).

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children and adults are at risk of online abuse.
- Children and adults can abuse their peers and others 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.

The School will also help employees to:

- develop better awareness to assist in spotting the signs and symptoms of online abuse

- develop the ability to ensure pupils and adults can recognise the dangers and risks in online activity and can weigh up the risks
- 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 will undertake child protection and safeguarding training, which will include online safety in accordance with statutory and Hampshire County Council policy. Alongside the Designated Teacher for Online Safety, 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, when applicable.

All training will follow the most recent Keeping Children Safe in Education publication.

12. Monitoring arrangements

The DSL (delegated to the Designated Teacher for Online Safety) will log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL, Senior Leaders and the Governing Body. The review will consider and reflect the risks pupils and adults face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This Policy will be applied alongside other relevant school policies as approved by Governors and published on our School's website.

<u>Rotherly Day Nursery variations include:</u>

Digital Safety is highlighted to Nursery children in an age-appropriate way through explicit teaching and day to day interactions. Useful information regarding digital safety is shared with parents regularly.

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

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS, INTERNET, DEVICES AND, PERSONAL MOBILE DEVICES ON SITE: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
When joining The Westgate School community, parents, carers and pupils agree to adhere to this policy. Agreement is made at the point of a child being admitted on roll to The Westgate School. **I will read and follow the rules in the acceptable use agreement policy; I will:** • Always use the School's IT systems and the internet responsibly and for educational purposes only • Only use them with the permission of an adult working in school • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it • Never use the device to take photos, film or record others without their permission **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking they are safe • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will only use it during lessons and only with the permission of the adult supervising/teacher for the purposes of learning • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online • I accept that the School will confiscate the device without negotiation if I break these rules **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**
Parent/carer's agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the School's IT systems and internet, and for using personal electronic devices in school and in outside of school in any way that is linked to the school, the school community or adults and pupils in school. I agree to use and model the use of online communication and technology in such a way that it does not fall within the realms of the Malicious Communications Act, 1998; I will make sure my child understands and adheres to these.

Appendix 2: Malicious Communications – Police Factsheet

ARE YOU THE VICTIM OF MALICIOUS COMMUNICATION?

A SELF-HELP GUIDE

CYBER CRIME ALERT

HAMPSHIRE CONSTABULARY

Malicious communication relates to the sending of indecent, offensive or threatening letters, electronic communication or articles with the intent to cause the recipient distress or anxiety.

If you are a victim of malicious communication there are steps you can take to stop the behaviour of the other person. These are detailed below.

OFFENDING BEHAVIOUR VIA ELECTRONIC & WRITTEN COMMUNICATION MAY INCLUDE BUT IS NOT LIMITED TO:

COMMUNICATION METHOD	+	THE CONTENT	=	A CRIME
		• Content grossly offensive, vulgar, outrageous, shameful, shocking, abusive, insulting • That is indecent, degrading, humiliating, improper, especially in relation to sexual matters • That is of a threatening nature and the threat is believed to be real • That is sent using false information that is believed to be false by the sender • Sent to cause the person or anyone else distress or anxiety		

ADVICE

- Ask the offender to STOP and then do not communicate any further
- Do NOT delete correspondence - keep copies of conversations by saving emails or taking screenshots
- REPORT any threatening, offensive or indecent content to the host website/platform
- BLOCK or unfriend those making unwanted contact - refer to host website/platform or Get Safe Online link below for assistance
- Do NOT retaliate – arguments will only continue and make it hard to determine who is at fault
- Seek SUPPORT from agencies such as Victim Support or the Samaritans if you need to talk about the impact the situation is having on your life

FURTHER SUPPORT

Victim Support: **www.victimsupport.org**
Samaritans: **www.samaritans.org**
Get Safe Online: **www.getsafeonline.org**

Appendix 3: The Westgate School's email protocol

*In order to **support all colleagues in work life balancing** and, to **nourish our harmonious working environment**, the Inside Out team has (in consultation with colleagues), devised the following email protocols to be followed, please.* ***Safeguarding is an exception to some of the protocols below.***

1. Automated response to **external emails** (aiming to manage expectations of pace):

   Thank you for contacting The Westgate School. This is an automated response to acknowledge safe receipt of your email.

   We endeavour to respond to emails within three school working days from receipt. This is because the matter may need investigation or indeed, because colleagues are engaged in teaching/working with pupils.

   If your concern pertains to a matter of child safety, please do not hesitate to call the School Office (01962 854757) asking to speak to:
   - *your child's Year Leader (Upper School);*
   - *Mrs. Fyvie-Rae (Designated Safeguarding Lead all-through);*
   - *Mrs. Williams (Lower School);*
   - *Mrs. Wild/Mrs. Christian (Headteacher's PA);*
   - *Alternatively, please re-send the email using CHILD SAFETY as the title.*

   We appreciate your understanding and partnership.
   The Westgate School.

2. **First principle: right person, right time, right place.**
3. **Email should not be used as a form of line management:** it is a tool for information requests or sharing.
4. Please **always try to talk to the person**: emails should be avoided where possible (eg use operational/Year Team faculty briefings).
5. Try to **avoid sending messages that expect a response during the day** as colleagues will be teaching.
6. Please use the **Colleague and Pupil Dashboards** for generic information (please don't put "tomorrow" as it is ambiguous…be date and space specific).
7. Internal emails: (unless it is a safeguarding or urgent communication) **not to be sent between 5.30pm on a Friday and 7.30am on a Monday morning** (extends to holidays, too).
8. Please **don't assume or expect** that colleagues will be checking emails in the evenings.
9. Please also be mindful of sending **work-related text messages**; sharing information (such as a reminder to your team leader that you are out) is a short, helpful communication *rather than* things that require action or thought!
10. When **sending an internal email**:
    - FAO: Teachers of X
    - Specify intended recipients when the email group doesn't currently exist eg PPG Mentors
    - No pupil lost property emails (it all goes to the medical room)
11. **Avoid "respond to all"** emails where everybody responds to a thread…
12. **Keep emails collegiate in tone and always mindful of the warm blooded person at the end**
13. Please **don't send emails to criticise somebody/something:** right person, right time, right place.
14. If it's **urgent, use a pupil** to send a message.
15. **Missing child emails are important** – delete if you can't help; please reply if you can.

16. Do **not set up automatic replies**.
17. **Colleagues do not have to accept habitual and vexatious emails from parents/carers**: if you receive these, please notify the Headteacher and we will support you.
18. **Try to avoid attachments where possible,** including key information in the text of the email.

WhatsApp Groups at Westgate School

Colleagues are welcome to belong to a social WhatsApp group for their department; however, this is optional and not an expectation. It can also be used for quick information sharing for those colleagues who choose to use it. However, this must not disadvantage anybody who does not wish to use WhatsApp. Information sharing should be avoided at weekends and during the holidays so that colleagues don't find it intrusive.

Colleagues should avoid using any colleague or pupil names; they must be aware that WhatsApp is open to Subject Access Requests and therefore, nothing potentially harmful must be said about individuals or the school on WhatsApp. Only when absolutely necessary to use as a tool for co-ordinating a response to a situation (eg Year Leaders), is it acceptable to use a pupils' initials.