THE WORTHGATE SCHOOL
CANTERBURY

ONLINE SAFETY POLICY

Date of Policy	August 2024
Reviewer(s)	Director of Safeguarding, Mental Health, and Wellbeing (DSL) Assistant Principal Academic Assistant Principal Pastoral
Approved by	Principal
Next Review Date	August 2025

THE WORTHGATE SCHOOL
CANTERBURY

Contents

Foreword

The educational and social benefits for students in using the internet should be promoted, but this should be balanced against the need to safeguard students against the inherent risks from internet technology. Further, the school needs to be able to teach students how to keep themselves safe whilst on-line. This is particularly important given that students predominantly access the internet through their own providers, which means that the school cannot apply filtering. The Online Safety Act 2023 is a significant piece of legislation in the UK aimed at enhancing online safety for both children and adults and this policy will align to key element within an educational setting.

Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole school community, including teachers, boarding staff, governors and others, and forge links with parents and the sales team. The strategy should be overseen by the Principal and be fully implemented by all staff, including operations and non-teaching staff.

Principal's Role

The Principal must have ultimate responsibility for online safety issues within the school including:

- the overall development and implementation of the school's online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community
- linking with the board of governors and parents and sales team to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and students who are in breach of acceptable use policies and responding to serious incidents involving online safety

Governors' Role

Governing bodies have a statutory responsibility for student safety and should therefore be aware of online safety issues, providing support to the Principal in the development of the school's online safety strategy.

Governors should ensure that there are policies and procedures in place to keep students safe online and that these are reviewed regularly. Governors should have appropriate safeguarding training to allow them to do this.

Governors should liaise with IT staff and service providers to annually review school IT filtering and monitoring systems to check their effectiveness and ensure that the school leadership team are aware of what provision is in place and how to escalate any concerns.

Governors should be subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct.

In particular, governors should always use business email addresses when conducting school business.

Online Safety Lead's Role

The school's designated Online Safety Lead (OSL) is the Designated Safeguarding Lead DSL, who is responsible for managing the online safety policies and documents on behalf of the school.

The OSL should have the authority, knowledge and experience to carry out the following:

- develop, implement, monitor and review the school's online safety policy
- ensure that staff and students are aware that any online safety incident should be reported to them
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, governors, students and parents regarding how to keep safe online
- liaise with the school's network manager, the Principal and nominated Safeguarding Governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems and that the school has appropriate filtering and monitoring systems
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers and complete the Filtering and Monitoring Risk Assessment annually
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated through PSHE
- ensure that all staff and students have read and signed the Acceptable Use Agreement (AUA)
- report annually to the board of governors on the implementation of the school's online safety strategy

The log of internet related incidents and co-ordination of any investigation into breaches will be maintained and led by the DSL.

Director of IT's Role

- the maintenance and monitoring of the school internet system including anti-virus and filtering systems (Fortinet)
- Ensuring that filtering and monitoring systems are robust and comply with the Department of *Education Filtering and monitoring standards for schools and schools*.

Meeting digital and technology standards in schools and schools - Filtering and monitoring standards for schools and schools - Guidance - GOV.UK (www.gov.uk) and with Keeping Children Safe In Education (KCSiE) 2024

- carrying out monitoring and audits of networks and reporting breaches to the DSL
- supporting any subsequent investigation into breaches and preserving any evidence

Role of School Staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for students. Their role is:

- adhering to the school's online safety and acceptable use policy and procedures
- communicating the school's online safety and acceptable use policy to students
- keeping students safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the DSL
- recognising when students are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the DSL
- teaching the online safety and digital literacy elements of the new curriculum

Designated Safeguarding Lead (DSL)

Where any online safety incident has serious implications for the child's safety or well-being, the matter should be referred to the DSL for the school who will decide whether a referral should be made to local Safeguarding Board, Front Door or directly to the Police.

Working with Parents and Carers

It is essential that the school involves parents and the student recruitment team in the development and implementation of online safety strategies and policies; most students will have internet access at home or their own mobile devices and might not be as closely supervised in its use as they would be at the school.

Therefore, parents and the sales team need to know about the risks so that they can continue online safety education at home and regulate and supervise students use as appropriate to their age and understanding.

The Principal, board of governors and the OSL/DSL should consider what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home.

Filtering & Monitoring

In accordance with The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education", the Worthgate School ensures that appropriate filtering and monitoring systems are in place to reasonably limit children's exposure to the risks from the school's IT system. As part of this process, the school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. Senior Leadership Team (SLT) and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified, as part of their roles and responsibilities.

The day-to-day management of filtering and monitoring systems requires the specialist knowledge of both Safeguarding and IT staff at the school to be effective. The DSL will have lead responsibility for safeguarding and online safety and the Director of IT services will have technical responsibility

Filtering

Worthgate school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for Schools and Colleges (2022) and the guidance provided in the UK Safer Internet Centre Appropriate filtering. In doing so:

- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details)
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon
- the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice under the Acceptable Usage Agreement (AUA)
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice

Monitoring

The Worthgate school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention and supported by the DSL
- Management of serious safeguarding alerts is consistent with Worthgate's Child Protection and safeguarding policy and practice

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed by the DSL and breaches are reported to the Principal
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention and support

Teaching Online Safety

Responsibility

One of the key features of the school's online safety strategy is teaching students to protect themselves and behave responsibly while on-line. There is an expectation that over time, students will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the Principal and the OSL, but all staff should play a role in delivering online safety messages
- The OSL is responsible for ensuring that all staff have the knowledge and resources to enable them to carry out this role
- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum
- Rules regarding safe internet use should be posted up in all classrooms and teaching areas where computers are used to deliver lessons
- The start of every lesson where computers are being used should be an opportunity to remind students of expectations on internet use and the need to follow basic principles to keep safe

- The school is required to teach about online bullying as part of Relationships and Sex Education and health education
- PSHE lessons provide an ideal space for discussion on online safety issues to ensure that students understand the risks and why it is important to regulate their behaviour whilst on-line
- Teachers should be aware of those students who may be more vulnerable to risk from internet use, generally those students with a high level of experience and good computer skills but coupled with poor social skills for example students with SEND.
- Teachers should ensure that the school's policy on students' use of their own mobile phones and other mobile devices in school is adhered to

Content

Students should be taught all elements of online safety included in the computing curriculum so that they:

- 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
- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- are responsible, competent, confident and creative users of information and communication technology

Students should be taught all elements of online safety included in statutory Relationships and Sex Education (RSE):

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders to report bullying and how and where to get help
- 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 students (including those created by students) is a criminal offence which carries severe penalties including jail

- That making, posting or sharing pictures of nude or semi-nude of students (including themselves) online is a criminal offence
- how information and data is generated, collected, shared and used online

Statutory Health Education should include:

- the similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image, how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information 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

Safe Use of Technology

Internet and search engines

- When using the internet, students should receive the appropriate level of supervision for their age and understanding. Staff should be aware that often, the most computer-literate students are the ones who are most at risk
- Students should not be allowed to aimlessly "surf" the internet and all use should have a clearly defined educational purpose
- Despite filtering systems, it is still possible for students to inadvertently access unsuitable websites; to reduce risk, teachers should plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.
- Where teachers require access to blocked websites for educational purposes, this should be discussed and agreed with the OSL, who will liaise with the IT team for temporary access
  Staff should notify the OSL once access is no longer needed to ensure the site is blocked

Evaluating and Using Internet Content

Teachers should teach students good research skills that help them maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content

Safe Use of Applications

Whilst online, students and staff should be aware of the sites they visit and the content therein. Typical access would be:

- School email systems should be hosted by an email system that allows content to be filtered and allow students to send emails to others within the school or to approved email addresses externally
- Social networking sites such as Facebook, Instagram and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these would have limited use in the school, but students are likely to use these sites at home
- Online communities and forums are sites that enable users to discuss issues and share ideas on-line
- Chat rooms are internet sites where users can join in "conversations" on-line; Instant messaging allows instant communications between two people on-line. In most cases, students will use these at home although school internet systems do host these applications
- Gaming-based sites allow students to "chat" to other gamers during gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to students. Consequently, such sites should not be accessible via school internet systems

Safety Rules

These rules apply to the users within the Worthgate network:

- Access to and use of personal email accounts, unregulated public social networking sites, chat rooms or gaming sites on the school internet system is forbidden. This forms part of the filtering and monitoring process and is usually blocked to protect students from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses
- If the school identifies a clear educational use for emails or social networking sites and forums for on-line publishing, they should only use approved sites such as those provided by the IT service provider. Any use of these sites should be strictly supervised by the responsible teacher
- Emails should only be sent via the school internet system to addresses within the School system or approved external address. All email messages sent by students in connection with school business must be checked and cleared by the responsible teacher

- Where teachers wish to add an external email address, this must be for a clear educational purpose and must be discussed with the OSL who will liaise with the learning platform provider
- Student email addresses must not be published on the school website
- Students should be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender
- Students should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites
- All electronic communications should be polite; if a student receives an offensive or distressing email or comment, they should be instructed not to reply and to notify the responsible teacher immediately
- Students should be warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the school's Behaviour Policy and Safeguarding and Child Protection Policy. This should include any correspondence or contact taking place outside the school and/or using non-school systems or equipment
- Users should be aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored
- In order to teach students to stay safe online outside of school, they should be advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    - to only use moderated chat rooms that require registration and are specifically for their age group
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken
    - not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room

Students Own Mobile Devices

The majority of students are likely to have mobile phones or other devices that allows them to access internet services, and these can pose a major problem for the school in that their use may distract students during lessons and may be used for online bullying.

However, many parents prefer their students to have mobile phones with them to ensure their safety and enable them to contact home if they need to. Generally, use of personal mobile phones

or other devices should be forbidden in classrooms, unless used for educational purposes as directed by the teacher.

Responding to Incidents

Policy Statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the DSL in the first instance. All incidents, whether involving students or staff, must be recorded by the DSL on the online safety incident report form (**Appendix 1**)
- Where the incident or complaint relates to a member of staff, the matter must **always** be referred to the Principal for action or consideration given to contacting the LADO where this is appropriate. Incidents involving the Principal should be reported to the Managing Director for Schools
- The school's OSL should keep a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system and use these to update the online safety policy
- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the DSL, who will decide as to whether or not to refer the matter to the police and/or local Safeguarding Board and Front Door in conjunction with the Principal

Although it is intended that online safety strategies and policies should reduce the risk to students whilst on-line, this cannot completely rule out the possibility that students may access unsuitable material on the internet.

The school cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional Access of Inappropriate Websites

If a student or teacher accidently opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately (and calmly) close or minimise the screen.

Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

The incident should be reported to the DSL/OSL and details of the website address and URL provided.

The OSL should liaise with the network manager or learning platform provider to ensure that access to the site is blocked, and the school's filtering system reviewed to ensure it remains appropriate.

Intentional Access of Inappropriate Websites by a Student

If a student deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).

The incident should be reported to the DSL and details of the website address and URL recorded.

The DSL should liaise with the network manager or learning platform provider to ensure that access to the site is blocked.

The student's parents may be notified of the incident and what action will be taken.

The student will be reminded of the risks associated with such websites and material.

As part of online safety awareness and education, students should be told of the "no tolerance" policy for online bullying and encouraged to report any incidents to their teacher.

Students should be taught:

- to only give out mobile phone numbers and email addresses to people they trust.
- to only allow close friends whom they trust to have access to their social networking page
- not to send or post inappropriate images of themselves
- not to respond to offensive messages
- to report the matter to their parents and teacher immediately

Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Any action taken on online bullying incidents must be proportional to the harm caused. For some cases, it may be more appropriate to help the students involved to resolve the issues themselves rather than impose sanctions.

Action by Service Providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. Teachers or parents can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The student should also consider changing their phone number
- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The student should also consider changing email address

- Where bullying takes place in chat rooms or gaming sites, the student should leave the chat room or gaming site immediately and seek advice from parents or teachers
- Bullying should be reported to any chat room moderator to take necessary action
- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked
- Parents should be notified of any incidents (where appropriate) and advised on what measures they can take to block any offensive messages on computers at home.

Harmful Sexual Behaviour and Child-on-Child Abuse Online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases, these actions may be harmful or abusive or may constitute harassment or online bullying.

Staff should be aware of online behaviours of a sexual nature that could constitute harmful behaviour:

- sharing explicit and unwanted content and images
- Consensual and non-consensual taking and distributing of inappropriate images (nude and semi-nude) of a young person (sexting)
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats
- coercing others into sharing images or performing acts online that they are not comfortable with.

Staff should be aware of their duty under statutory guidance *Keeping children Safe in Education* and *Sexual violence and sexual harassment between students in Schools and schools* which requires the school to have policies in place to deal with incidents of on-line sexual harassment.

Schools should also be aware of when any of these behaviours may be linked to extra-familial harm such as the criminal or sexual exploitation of a student or is being carried out as a gang-related activity.

If a member of staff becomes aware of any such harmful behaviour, it should be reported immediately to the DSL.

Risk From Inappropriate Contacts With Adults

Teachers may be concerned about a student being at risk because of their contact with an adult they have met over the internet. The student may report inappropriate contacts or teachers may suspect that the student is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of students being sexually abused on-line through video messaging platforms such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the DSL
- The DSL should discuss the matter with the referring teacher and where appropriate, speak to the student involved, before deciding whether or not to make a referral to Local Safeguarding and Front Door and/or the police
- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school
- The DSL can seek advice on possible courses of action from KCC's online safety officer in Local Safeguarding and Social Work
- Teachers will advise the student on how to terminate the contact and change contact details where necessary to ensure no further contact
- The DSL/OSL should consider notifying the student's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety
- Where inappropriate contacts have taken place using school IT equipment or networks, the OSL should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other students is minimised

Risk From Contact With Violent Extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts.

Because of their personal circumstances, some young people may be susceptible to these influences and may be radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All staff have a duty under the Government's *Prevent* programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is the Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff need to be aware of the school's duty under the *Prevent* programme and be able to recognise any student who is being targeted by violent extremists via the internet for the purposes of radicalisation. Students and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies
- The school should ensure that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism

- All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate
- The designated safeguarding lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue
- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, staff should refer the matter to the DSL who will refer the young person to the MASH

Risk From Sites Advocating Suicide, Self-Harm and Anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- The school should ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PSHE curriculum
- Pastoral support should be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor
- Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help

Appendix 1: Key Contacts

School Contacts

Name of School:

Worthgate School Canterbury

Principal:

Ian Gross

Online Safety Lead (OSL):

Martyn Rogers mrogers@worthgateschool.com

IT systems/Data manager:

Wayne Creighton wcreighton@catsglobalschools

Designated Safeguarding Lead (DSL):

Martyn Rogers mrogers@worthgateschool.com

Nominated Safeguarding Governor:

Craig Wilson (crwilson@catsglobalschools.com)

Education Safeguarding Service Contacts

Head Office: Room 2.30 Sessions House, County Hall, Maidstone, ME14 1XQ	
Claire Ray Head of Service	**03000 423 169**
Rebecca Avery Training & Development Manager	**03000 423 168**
Robin Brivio Senior Safeguarding Advisor	**03000 423 169**
Ashley Assiter (Mon - Weds) Online Safety	**03000 423 164**

For advice on safeguarding issues please call your area office on the numbers listed below. **If a child may be at risk of imminent harm, you should call the Integrated Front Door on 03000 411111 (frontdoor@kent.gov.uk) or the Police on 999**	
Ashford	**03301 651340**

Canterbury	**03000 423 157**
The Education People Consultation Line	**03000 423 157**
Dartford	**03000 423 149**
Dover	**03000 423 154**
Folkestone & Hythe	**03000 423 154**
Gravesham	**03000 423 149**
Maidstone	**03000 423 158**
Sevenoaks	**03000 423 149**
Swale	**03000 423 157**
Thanet	**03000 423 157**
Tonbridge & Malling	**03000 423 158**
Tunbridge Wells	**03301 651440 03000 423 158**

Kent Education Safeguarding Advisors

- Myles O'Keeffe
- Anup Kandola
- Kirstie Owens
- Gemma Lawford
- Gemma Willson (Monday/Tuesday)
- Claire Ledger (Wednesday/Thursday/Friday)

Kent County Council Key Contacts

- **Integrated Front Door**: **03000 411111** (outside office hours **03000 419191)**
- **Early Help Contacts** (district teams) can be found on www.kelsi.org.uk
- **LADO Team contact number: 03000 410888**

If your call is urgent I.e. a child is in immediate danger and you cannot be connected to the team, you should call the Integrated Front Door on Phone: **03000 411111**

Email: Frontdoor@kent.gov.uk
Kroner House, Eurogate Business Park, Ashford. Kent TN24 8XU

Prevent Education Officers

North/West/ Medway – Sally Green sally.green2@kent.gov.uk 03000 413439
South/East – Rachel Murray Rachel.Murray@kent.gov.uk 03000 413565

Appendix 2 - Online Safety Incident Report Form

Name of School/organisation:	Worthgate School
Address:	68 New Dover Road, Canterbury CT1 3LQ
Name of Online Safety Lead (OSL):	Martyn Rogers
Contact details:	mrogers@worthgateschool.com 07794 087422 and 01227 378378

Details of Incident

Date happened:	
Time:	
Name of person reporting incident:	
(If not reported, how was the incident identified?)	
Where did the incident occur?	□ In school/service setting
	□ Outside school/service setting
Who was involved in the incident?	□ child/young person
	□ staff member
	□ other (please specify below)
Type of incident:	□ bullying or harassment (online bullying)
	□ deliberately bypassing security or access
	□ hacking or virus propagation
	□ racist, sexist, homophobic, transphobic, bi-phobic, religious hate material
	□ terrorist material
	□ online grooming
	□ online radicalisation
	□ child abuse images
	□ on-line gambling
	□ soft core pornographic material
	□ illegal hard core pornographic material
	□ other (please specify below)

Description of Incident

Nature of Incident

□ **Deliberate Access**	
Did the incident involve material being:	□ Created
	□ Viewed
	□ Printed
	□ Shown to others
	□ Transmitted to others
	□ Distributed
Could the incident be considered as:	□ harassment
	□ grooming
	□ online bullying
	□ breach of AUP
□ **Accidental Access**	
Did the incident involve material being:	□ Created
	□ Viewed
	□ Printed
	□ Shown to others
	□ Transmitted to others
	□ Distributed

Action Taken

□ **Staff**	□ incident reported to Principal/SLT
	□ advice sought from LADO
	□ referral made to LADO
	□ incident reported to police
	□ incident reported to Internet Watch Foundation
	□ incident reported to IT
	□ disciplinary action to be taken
	□ online safety policy to be reviewed/amended
	Please detail any specific action taken (i.e.: removal of equipment, below)

□ **Child / Student / Young Person**	□ incident reported to Principal/SLT
	□ advice sought from Students Safeguarding and Social Work
	□ referral made to Students Safeguarding and Social Work
	□ incident reported to police
	□ incident reported to social networking site
	□ incident reported to Internet Watch Foundation
	□ child's parents informed
	□ disciplinary action to be taken
	□ child/young person debriefed
	□ online safety policy to be reviewed/amended
	Please detail any specific action taken (i.e.: removal of equipment, below)

Outcome of Incident / Investigation
