Kingsmead School & Sixth Form

Online Safety Policy

This plan is reviewed annually in the autumn term.

Next Review Due: June 2027

History of Document:

Issue No.	Date Issued	Prepared By	Approved By	Comments
Issue 1	Nov 2023	G Clare	TB Nov 2023	Policy formatted
Issue 2	Sept 2024	G Clare	TB Dec 2024	Updated
Issue 3	May 2027	G Clare	TB June 2026	Logistical updates

Contents

1. Aims 3
2. Legislation and guidance 4
3. Links with other policies 5
4. Roles and responsibilities 5
5. Educating pupils about online safety 7
6. Artificial Intelligence (AI) 9
7. Educating parent/carers about online safety 9
8. Cyber-bullying 10
9. Acceptable use of the internet in school 11
10. Filtering and monitoring 11
11. Mobile devices in school 12
12. Remote learning 12
13. Staff using work devices outside school 13
14. How the school will respond to issues of misuse 13
15. Training 13
16. Monitoring arrangements 14
Appendix 1: Online safety training needs – self audit for staff 15
Appendix 2: Online safety incident report log 16
Appendix 3: Acceptable Usage Policy for the Computer System & Internet 17

1. Aims

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers Kingsmead to protect and educate children and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

All staff receive intensive safeguarding training at the start of the academic year and when they join Kingsmead school. It is made explicitly clear to staff that it is everyone's responsibility to ensure our children are safe when working online. We ensure that our online safety policy recognises and informs the different requirements of our learners in terms of age, role and need.

Alongside extensive training for staff, our children receive online safety lessons as part of the Character Curriculum and Computing/IT lessons and our parents receive the option to attend training, or watch training on the school website, to learn how to protect their families using their own Wi-Fi security system at home.

This policy incorporates the schools acceptable use procedures. Online safety and acceptable use are closely linked because both aim to protect students, staff, and the school community when using digital devices and the internet. Online safety focuses on preventing risks such as cyberbullying, scams, and exposure to harmful content, while acceptable use sets clear rules for responsible behaviour, like keeping passwords secure, using devices for learning, and reporting suspicious activity. By following the acceptable use, students and staff put online safety principles into practice, ensuring a secure, respectful, and productive digital environment for everyone.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and trustees.
- 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 breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

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.

As further explained in section 9 of this policy, filtering and monitoring systems are in place at Kingsmead to protect our children from accessing inappropriate or harmful content. Should a child attempt to access such sites the Designated Safeguarding Lead/Safeguarding team will be alerted via the online monitoring system, Smoothwall, and subsequent action put into place to both protect and educate the child.

- **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.

Students are not permitted to have their mobiles phones while at school. If their phone is confiscated by school staff, it is not returned until 5 working days. This works well to deter students from using their phones and social media accounts during the school day which in turn prevents unwanted incidents after school. Students are further educated about the impact of negative social media use and how this affects others and put themselves in danger. This is taught through several platforms such as IT/computing lessons, safeguarding assemblies, and our Character curriculum.

- **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.

Students are taught how easy it is to get involved in negative conduct online. For example, how being part of a large whatsapp group where someone else shares an explicit image or where other people bullying someone in the group can result in serious consequences for all students involved. They are also taught about the impact of sharing an explicit image and how it can go wrong quickly.

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Such sites are blocked by Smoothwall at school and students are provided with information on how to keep themselves safe and what to look out for.

6th form lap tops are monitored on and offsite when they are connect to WiFi. Alerts are received via Smoothwall.

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. Links with other policies

This online safety policy is linked to our:

- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

4. Roles and responsibilities

4.1 The Trustees

The Trustees have overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Trustees 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 Trustees will ensure online safety is a running and interrelated theme whilst devising and implementing their whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role, and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

The trustee who oversees online safety is Usman Haroon`.

All Trustees 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
- 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.

4.2 The headteacher

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

4.3 The designated safeguarding lead

Details of the school's DSL and Deputy DSL are set out in our child protection and 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, network manager and other staff, 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 and behaviour 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 staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Trustees.

This list is not intended to be exhaustive.

4.4 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 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 a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Recording the sites/categories that are blocked and ensuring this is age appropriate and does not over block the system
- 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 dealt with appropriately in line with the school behaviour policy.
- Working with the DSL to oversee the filtering and monitoring guidelines outlined in the digital standards.

This list is not exhaustive.

4.5 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 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.

4.6 Parent/carers

Parent/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents 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

4.7 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.

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. As stated previously, safety is taught explicitly through the Character Curriculum and Computing/IT curriculum which includes:

- Positive online interactions and ensuring safe interactions.
- Treating each other with respect online.
- Managing digital footprints on a variety of social media platforms.
- Laws regulating sexting.
- Identifying and reporting online banter, abuse, harassment, and bullying
- Consequences for abusive or unsafe online behaviours.
- Media literacy and social media literacy.
- What constitutes sexual harassment and how to report it.
- The positives and consequences of Artificial Intelligence

This policy works in conjunction with the Safeguarding and Child Protection Policy

A safeguarding assembly is delivered to all year groups which outlines how to keep safe online and how/where to seek help.

An Online safety, online profiles and social media presentation is delivered to all year groups during assembly by the Head of Year.

The School of Sex Education delivers presentations to pupils during termly drop-down days.

Pupils will be spoken to by the BfL team/HOY if they are involved in incidents concerned with online safety.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

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

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.
- The above will be covered in the Year 7 and 8 Computing curriculum.

In **Key Stage 4** pupils will be taught to:

- 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.
- The law and how their actions could result in Police intervention.
- 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).

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

6. Artificial Intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Microsoft Co-pilot.

Kingsmead 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Kingsmead School will treat any use of AI to bully pupils very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

6.1 Ethical and responsible use

We will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our school's equality policy when using generative AI tools
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

7. Educating parent/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be on our website.

Parents are also invited to attend parent coffee mornings, evening presentations and online webinars with the Parent Support Advisor (PSA) and Online Safety Lead.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

8. Cyber-bullying

7.1 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 behaviour policy.)

7.2 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 that they can report any incidents to any teacher or by visiting BfL to write a statement. Pupils 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. This takes place during tutor time and character curriculum lessons.

All staff, Trustees, 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.

If a crime has been committed the school will contact 101 or Report a Crime Online.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads, and other tablet devices, 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
- Disrupt teaching, and/or
- Break any of the school rules

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 whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* *Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.*

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

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

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

9. Acceptable use of the internet in school

All pupils, parents, staff, volunteers, and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. 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, trustees and visitors (where relevant) to ensure they comply with the above.

10. Filtering and monitoring

Schools are required "*to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering*". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "*ensure appropriate filters and appropriate monitoring systems are in place and regularly review their effectiveness" and they "should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system*" however, schools will need to "*be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.*" Ofsted concluded as far back as 2010 that "Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves." (UK Safer Internet Centre)

Kingsmead school uses Smoothwall to filter and monitor pupil and staff internet use. The programmes are reviewed termly to ensure their effectiveness. The senior leadership team and Designated Safeguarding Lead have an awareness of the systems in place and manage them effectively and know how to escalate concerns when identified.

To ensure we are meeting this duty, we follow the filtering and monitoring standards set out by the Department for Education and guidance from the UK Safer Internet Centre.

The standards set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.

- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

When deciding the appropriateness of the level of filtering and monitoring the school considers the age range of the pupils, the number of pupils, how often they access the IT system and the proportionality of costs versus safeguarding risks. Staff will consider the vulnerabilities of the cohort, for example students with SEND/Educational Health Care Plans might be more susceptible to online risks and require further education and/or monitoring.

The DSL works closely with the network team to make sure that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regard to online teaching and safeguarding. If teachers wish to access a site that is blocked, they can contact network and the DSL who liaise with the teacher to decide if the site can be unblocked for a set period.

11. Mobile devices in school

Kingsmead school follows a strict behaviour policy which all pupils are expected to adhere to. As part of this policy there is a no mobile phone use policy. Pupils are not permitted to have a mobile on their person at any time. If a pupil is found to have a mobile phone it is confiscated and kept in school for 5 calendar days. An adult must then come into school to collect the mobile.

Pupils in the 6th form may use them in designated areas of the school and may use them in some lessons at the discretion of the teacher as long as they are flat on the desk.

Staff are not permitted to use their mobile phones when in charge of students. All mobile phone use must take place privately. Staff are not permitted to take photos using their mobile phone device of students.

12. Remote learning

Keeping pupils and teachers safe during remote education is essential. Teachers delivering remote education online are aware that the same principles set out in the school policies apply to remote education as well.

All lessons follow the same procedure that would normally take place in the classroom as far as possible. Teachers record their lessons to ensure everyone's safety. Teachers will follow the normal protocol for reporting concerns to the Designated Safeguarding Lead (DSL) as they would if they were on school site. The safe@kingsmead.org email address is regularly shared with all parties during school closure to ensure clear lines of communication for reporting any safeguarding concerns.

School laptops are monitored by Smoothwall which alerts the DSL to any activity which might be of concern. This continues when the laptop is being used outside of school.

This section summarises our approach to remote learning. For comprehensive details about our school's policy on remote learning, please refer to our remote learning policy which you can find on our website.

13. 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).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- 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.

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.

14. 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 policies on Behaviour and ICT and internet acceptable use. 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. 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.

15. 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.
- Children 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 deputies will undertake Child Protection training. The DSLs and Senior Leadership Team 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.

Trustees 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.

16. Monitoring arrangements

Any member of staff may log behaviour and safeguarding issues related to online safety on CPOMs.

This policy will be reviewed **annually** by Gemma Clare, DSL. At every review, it will be approved by the full governing board. The policy will be ratified at the Pastoral Trustee meeting and shared and implemented by the safeguarding team. All stake holders will be made aware of the updated policy, and it will be shared on the school website for parents, visitors, volunteers, and temporary staff to access.

The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

An online safety audit will be completed annually using a recognised assessment tool.

Appendix 1: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: Online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 3: Acceptable Usage Policy for the Computer System & Internet

You must abide by these rules when using the Computer System, Internet and sending emails.

I will only use my own network and login and password, which I will keep private at all times.

I will only look at, change, or delete my own files.

I understand that I must not bring software or disks into school without permission.

If I see anything I am unhappy with or I receive a message I do not like, I will tell a teacher immediately.

I understand the school has the right to check my computer files, the Internet sites that I visit and the public areas of social networking sites in order to investigate incidents of Malicious Communications.

I will only email people I know, or a member of staff as approved.

The email messages I send will be polite and sensible.

I will ask permission before opening an email or an email attachment sent by someone I do not know.

I understand that I must never give my home address or telephone number or arrange to meet someone over the internet.

I will not use Internet chatrooms except as instructed by my teacher.

I will not use the school's computer system to download games or other materials deemed inappropriate by the school.

I will not make any attempt to harm the school's ICT system. This may include, but is not limited to, the uploading of viruses, willful damage of hardware and deletion of data from its place of storage.

I understand that if I break these rules, I may not be allowed to use the Internet or computers and may face more serious sanctions; my parents will be contacted and informed of my behaviour.

Should my parents not wish to allow me access to the Internet then they must inform the school in writing.

I have read and understood the Kingsmead School Acceptable User Policy.

Signed_____**(Pupil)**

Signed_____**(Parent/Carer)**