WOODSIDE

Online Safety Policy

Last reviewed in: February 2019
Accepted by Trustees in: September 2021
Due for next review in: September 2022

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating children about online safety 5
5. Educating parents about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 7
8. Children using mobile devices in school 7
9. Staff using work devices outside school 7
10. How the school will respond to issues of misuse 8
11. Training 8
12. Monitoring arrangements 9
13. Links with other policies 9
Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers) 10
Appendix 2: KS2, KS3 and KS4 acceptable use agreement (children and parents/carers) 11
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 12
Appendix 4: online safety training needs – self audit for staff 15
Appendix 5: online safety incident report log 16

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors
- 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, racism, self-harm, suicide, 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 scam.

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 children' 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.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trustee Board

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

The Trustee Board 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 link trustees for safeguarding in our school are Karen Kempster and Gill Jones.

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 (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some children 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.

3.2 The headteacher

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

3.3 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 job descriptions.

The DSL (at Woodside this is the headteacher) takes lead responsibility for online safety in school, in particular:

- ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the ICT 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

- ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the Trustee Board.

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT 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 children 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 regular 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 (see appendix 5) 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.

This list is not intended to be exhaustive.

3.5 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 (appendix 3), and ensuring that children follow the school's terms on acceptable use (appendices 1 and 2)
- working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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.

3.6 Parents and carers

Parents and 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 (appendices 1 and 2)

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

3.7 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 (appendix 3).

4. Educating children about online safety

Children will be taught about online safety as part of the curriculum.

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the 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.

In **Key Stage 1**, children 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.

Children 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**, children 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.

The safe use of social media and the internet will also be covered in other subjects where relevant.

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

5. Educating parents and 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 shared with parents.

Online safety will also be covered during parents' workshops when applicable.

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.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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 behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class.

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

All staff, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support children, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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 children, the school will use all reasonable endeavours to ensure the incident is contained.

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.

6.3 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 children' 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 child discloses that they are being abused and that this abuse includes an online element.

Any searching of children 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
- The school's COVID-19 risk assessment.

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

7. Acceptable use of the internet in school

All children, parents, staff, volunteers and trustees are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). 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 children, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Children using mobile devices in school

Woodside School's policy relating to the use of devices such as mobile phones, is set out in the relevant AUP.

Children bringing in their own devices such as mobile phones and smart watches, should hand these in to the school office before each school day. Children found to be in breach of this requirement will have their device confiscated and sent to the school office in a sealed envelope marked with the child's name and class. Confiscated phones can be collected by parents/carers at the end of the school day.

Any breach of the acceptable use agreement by a child may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. 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
- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

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 Mark Owen, IT Technician.

10. How the school will respond to issues of misuse

Where a child misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, child protection and safeguarding, 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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 children can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence children 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 and 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.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the Trustee Board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks children 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 online safety policy is linked to our:

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

Appendix 1: EYFS and KS1 acceptable use agreement (children and parents/carers)

I want to feel safe all the time.

I know that anything I do on the computer can be seen by other people.

I know when to use the CEOP report button.

I agree that I will:

- not use my own mobile phone, or any other device, in school, unless I am given permission
- always keep my passwords safe and not share them with anyone
- only open web pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or unhappy on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel sad or worried
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home,
- my family or my pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger.

Signed (parent/carer)_____Date _____

Pupil name _____

Signed _____Date _____

Appendix 2: KS2 acceptable use agreement (children and parents/carers)

When I am using the computer or other technologies, I want to feel safe all the time.

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored by school.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will:

- always keep my passwords safe and not share them with anyone
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved, and I will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe, worried or uncomfortable
- not reply to any nasty message or anything which makes me feel unhappy or worried
- not use my own mobile phone, or any other device, in school, unless I am given permission
- only give my mobile phone number to friends I know and trust in real life
- only email people I know or are approved by my school
- only use email which has been provided by school
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before creating a profile or signing up for an account
- always follow the terms and conditions when using a website
- always keep my personal details private. (My name, family information, journey to school,
- my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

Signed (parent/carer) _____ _____ Date _____

Pupil name _____Signed _____ Date _____

Appendix 3: acceptable use agreement (staff, trustees, volunteers and visitors)

- I understand that I have personal and legal responsibilities, including treating others with dignity and respect, acting honestly, using public funds and school equipment appropriately, adhering to health and safety guidelines and safeguarding pupils at all times.
- I understand that I must use school devices and systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of systems and other users.
- I recognise the value of the use of digital technology for enhancing learning and will ensure that children receive opportunities to benefit from the use and application of appropriate digital technology.
- I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with children and young people.

Professional and personal safety:

☐ I understand that the school has in place a filtering system and will monitor my access to digital technology and communications systems whilst using school devices, and/or access to the school network via personal devices, where such access has been granted.

☐ I understand that the rules set out in this agreement also apply to use of school devices and digital technologies out of school, and to the transfer of personal data (digital or paper based) out of school.

☐ I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use in line with the general principles of this agreement and the expectations of professional behaviour set out in the Staff Code of Conduct.

☐ I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should keep passwords safe and not share them with anyone.

☐ I will immediately report any incidence of access to illegal, inappropriate or harmful material, deliberate or accidental, by myself or others, to the appropriate person.

☐ I will not install or attempt to install programmes of any type on a device, nor will I try to alter computer settings, unless this is permitted by the Network Manager.

☐ I will not deliberately disable or cause any damage to school equipment, or the equipment belonging to others.

☐ I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy).

☐ I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when required by law, or by school policy, to disclose such information to an appropriate authority.

☐ I will immediately report any damage or faults involving devices or software, however this may have happened.

☐ I will ensure that I have permission to use the original work of others in my own work.

☐ Where work is protected by copyright, I will not download or distribute copies (including music and

videos).

☐ I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

☐ I will log out of a device when I have finished using it.

Electronic communications and use of social media:

☐ I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

☐ I will use social networking sites responsibly, taking care to ensure that appropriate privacy settings are in place, and ensure that neither my personal nor professional reputation, nor the school's reputation, is compromised by inappropriate postings, to include past postings.

☐ I will never send or accept a 'friend request' made through social media from a student at school. I understand that such requests should be raised formally as an incident.

☐ I will not, under any circumstances, make reference to any staff member, student, parent or school activity/event via personal social media or other communication technologies.

☐ I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner. At no time will I use or share a personal email address, phone number or social networking site for such communication purposes.

☐ I will notify the Headteacher of any current or future, direct or incidental contact with students, parents or carers, for example where parents or carers are part of the same social group

☐ I will not engage in any online activity, at, or outside school, that may compromise my professional responsibilities. This includes making offensive, aggressive or defamatory comments, disclosing confidential or business-sensitive information, or information or images that could compromise the security of the school.

☐ I will not use the school's name, logo, or any other published material without written prior permission from the Headteacher. This applies to any published material, online or in print.

☐ I will not post any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school.

Use of school and personal mobile devices and technologies:

☐ When I use my own mobile device (e.g. laptop / tablet / mobile phone / USB device) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

☐ I will keep my personal phone numbers private and not use my own mobile phone, or other device, to contact students or parents in a professional capacity.

☐ I will keep my mobile phone secure whilst on school premises. It will be switched off whilst I am on duty unless there are good reasons that have been approved with a member of the senior leadership team, and then that is discreet and appropriate, e.g. not in the presence of students.

☐ I will keep mobile devices switched off and left in a safe place during lesson times. I understand that the school cannot take responsibility for personal items that are lost or stolen.

☐ I will report any text or images sent to me by colleagues or students which could be viewed as inappropriate. I will not use a personal device to photograph a student(s), except with the written permission of the Headteacher.

☐ I will not use personal email addresses on the school ICT systems.

☐ I will not open any hyperlinks in emails or any attachments to emails if I have any concerns about the validity of the email or its source is neither known nor trusted.

☐ I will, when I take and/or publish images of others, do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use any personal devices to record these images, unless I have written permission from the Headteacher. Where these images are approved by the school to be published (e.g. on the school website) it will not be possible to identify by name, or any other personal information, those who are featured.

☐ I will not attempt to upload, download or access any material which is illegal (for example; images of child sexual abuse, criminally racist material, adult pornography), inappropriate or may cause harm or distress to others. I will not attempt to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

☐ I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

Conduct and actions in and out of the school:

☐ I understand that this Acceptable Use Policy applies not only to my work and use of school devices and digital technology in school, but also applies to my use of school systems and equipment off the premises. This Acceptable Use Policy also applies to my use of personal devices on the premises or in situations related to my employment by the school.

☐ I understand that should I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action in line with the school's agreed Disciplinary Procedure. In the event of any indication of illegal activity, I understand the matter may be referred to the appropriate agencies.

I have read and understood the above, and agree to use school devices and access digital technology

systems (both in and out of school), as well as my own devices (in school and when carrying out

communications related to the school), within this agreement.

I understand that in the event of any query or concern about this agreement, I should contact the Headteacher.

Staff/volunteer name:	
Signed:	
Date:	

Appendix 4: 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 children can abuse their peers online?	
Do you know what you must do if a child 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 children 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 5: 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**