THE ASHBY FEDERATION

ONLINE SAFETY POLICY

Approved by:	Executive Headteacher	**Date:** January 2022
Last reviewed on:	January 2022	
Next review due by:	January 2024	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial 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 pupils' electronic devices where they believe there is a 'good reason' to do so.

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

3. Roles and responsibilities

3.1 The Governing Body

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

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governors who oversee online safety are: -

Michael Boniface at Yardley Hastings Primary

Robert Mackenzie-Wilson at Denton Primary.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, 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

3.2 The Executive Headteacher

The Executive 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 and deputies

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 DDSL's **(Andy Baker – Yardley Hastings, Rosie Gibson – Denton) and the Computing Subject Lead (Amber Hayfield)** take lead responsibility for online safety in school, in particular:

- Working with 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 6) 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 5 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 Governing Body

This list is not intended to be exhaustive.

3.4 The ICT Technical Support Provider

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 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 fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL/DDSL to ensure that any online safety incidents are logged (see appendix 6) 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'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Executive 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 pupils about online safety

Pupils 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**, pupils will be taught to:

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

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

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

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

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

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 pupils with SEND.

5. Educating parents 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.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Executive Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the Executive 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 pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

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

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

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

The school does not allow pupils to bring into school mobile phones or personal electronic devices. In exceptional cases, the device should be handed into the school office for safe keeping, and collected at the end of the day.

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

7. 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 (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 pupils, 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. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure, as per the schools Code of Conduct. 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 EasiPC.

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, please see Appendix 4.

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

10. 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 deputy/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.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

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

11. Monitoring arrangements

The DSL/DDSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 6.

This policy will be reviewed every two years by the Executive Head Teacher. At every review, the policy will be shared with the Governing Body and done in conjunction with the outcome of the 360safe review. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff code of conduct
- Data protection policy and privacy notices
- ICT policy

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

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet.

In order to support the school in educating your child/young person about e-Safety (safe use of the Internet), please read the following Rules with your child/young person then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the E-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact the Executive Headteacher.

Yours faithfully,

Xxxxxxx

Online Safety Acceptable Use Rules Return Slip, 200x – 200x

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

EYFS and Key Stage 1

Our Internet and E-mail Rules

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password safely.
- We know who to ask for help.
- If we see something we do not like we will tell an adult immediately.
- We know that it is important to follow the rules.
- We will always log off the computer when we have finished using it.

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

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet.

In order to support the school in educating your child/young person about e-Safety (safe use of the Internet), please read the following Rules with your child/young person then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the E-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact the Executive Headteacher.

Yours faithfully,

Xxxxxxx

Online Safety Acceptable Use Rules Return Slip, 200x – 200x

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Key Stage 2

Our rules for using the Internet safely and responsibly.

- We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail or chat to people an adult has approved.
- Adults are aware when we go on-line and we know we are not allowed to do so without an adult in the room.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips to approved websites and with an adult's permission.
- If we need help we know who to ask.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we tell an adult immediately.
- If we receive a message sent by someone we don't know we do not open it until we have gained an adult's permission.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using our safe Internet in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.
- We will always log off the computer when we have finished using it.

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

These rules apply to all on-line use and to anything that may be downloaded or printed. To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, these rules will be discussed regularly at staff meetings and as part of the induction procedures. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse (Appendix 4) so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Executive Headteacher, or Deputy Designated Person(s) for Child Protection
- I know who my Designated Person(s) for Child Protection are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Executive Headteacher and/or DDSL.
- I know that I should complete virus checks on my laptop and encrypted memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the GDPR policy and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriately requests my password, I will check with DSL/DDSL.
- I have been given a copy of the Online Safety Policy to refer to about all online safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

Signed …….. Date …….

Print name ……

Appendix 4: procedures following misuse by staff or pupils

Staff Procedures Following Misuse by Staff

The Executive Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:

- Report website to the DSL/DDSL if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/Easi PC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Executive Headteacher (DSL) and DDSL immediately.
- Executive Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the LA/Easi PC filtering services as with A.
- Follow safeguarding procedures (in Child Protection and Safeguarding Policy)

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Executive Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Follow procedures detailed in the Child Protection and Safeguarding Policy

D. An adult has used ICT equipment inappropriately:

- Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Executive Headteacher and DSL immediately, who will follow procedures detailed in the Child Protection and Safeguarding Policy
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff, Staff Code of Conduct and Executive Headteacher to implement appropriate sanctions.
- If illegal or inappropriate misuse is known, contact the Executive Headteacher or Chair of Governors (if allegation is made against the Executive Headteacher) and DSL immediately and follow the Child Protection and Safeguarding Policy
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website about an adult in school:

- Preserve any evidence.
- Inform the Executive Headteacher immediately and follow Child Protection Safeguarding Policy as necessary.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information posted about them this should be report to the Executive Headteacher

N.B. There are three incidences when you must report directly to the police via the Multi Agency Safeguarding Hub (See Child Protection and Safeguarding Policy):-

- **Indecent images of children found.**
- **Incidents of 'grooming' behaviour.**
- **The sending of obscene materials to a child.**

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image. • www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line. **It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.**

Staff Procedures Following Misuse by Children and Young People

The Executive Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the DSL/DDSL if this is deemed necessary.
- Contact the helpdesk filtering service for school and Easi PC so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction, as per Behaviour Policy
- Notify the parent/carer.
- Inform Easi PC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Inform parent/carer
- Report to the Executive Headteacher and DSL immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Executive Headteacher must follow the Child Protection and Safeguarding Policy
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website about a child in school:

- Preserve any evidence.
- Inform the Executive Headteacher immediately.
- Inform parent/carer
- Inform Easi PC and DSL/DDSL so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Executive Headteacher immediately.

N.B. There are three incidences when you must report directly to the police via the Multi Agency Safeguarding Hub (See Child Protection and Safeguarding Policy).

- **Indecent images of children found.**
- **Incidents of 'grooming' behaviour.**
- **The sending of obscene materials to a child.**

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.

If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

• www.iwf.org.uk will provide further support and advice in dealing with

offensive images on-line.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Appendix 5: 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 6: 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**