LATCHMERE
ACADEMY TRUST

Online Safety Policy

Status	Statutory
Review Cycle	Annual
Date written/ last review	September 2022
Date of next review	September 2023

Contents

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, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the Department for Education's (DfE's) 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.

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

Roles and responsibilities

The trust board

The trust board has overall responsibility for monitoring this policy and holding the executive headteacher to account for its implementation.

School governors are directed by the trust board to co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

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

The designated safeguarding lead

Details of the school's designated safeguarding lead (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, 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 headteacher and/or governing board

This list is not intended to be exhaustive.

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 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
- 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.

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 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.

Parents

Parents 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

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).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

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

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.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

Cyber-bullying

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and DSL as set out in our behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

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

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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

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 to 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 to 3.

Official Use of Social Media

Latchmere Academy Trust's official social media channels are Twitter and Instagram.

● Official school social media channels will be set up as distinct and dedicated social media sites or accounts for educational or community engagement purposes only.

● Staff use school provided email addresses to register for and manage any official school social media channels.

● Official social media sites are suitably protected and, where possible, run and/or link from the school website.

● Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

Online safety and Acceptable Use of ICT

● Official social media use will be conducted in line with existing policies, including: Anti-bullying, Data protection, Safeguarding and Child protection (copies are available on the Policy Page of the Trust website).

● All communication on official social media platforms will be clear, transparent and open to scrutiny.

● The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

● Members of staff who follow and/or like the school social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

● If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:

● Be professional at all times and aware that they are an ambassador for the school.

● Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.

● Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.

● Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.

● Ensure that they have appropriate written consent before posting images of pupils, staff or others on the official social media channel.

● Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

● Not engage with any direct or private messaging with current, or past, pupils, parents and carers.

● Inform their line manager, the Designated Safeguarding Lead and/or the Head teacher of any concerns, such as criticism, inappropriate content or contact from pupils.

Publishing Images and Videos Online

● The schools in the Multi Academy Trust will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Data Protection Policy, Acceptable Use Agreements and the Staff Code of Conduct (copies available on the Policy Page of the Trust Website).

Naming Students

● DO NOT use students' names if a picture is being used. You may use class names and a photo.

● First names may only be used in the newsletter - you may re-tweet these or send a link to articles but may not use a student's name in social media post.

● If you wish to use a student's name in a social media post; winning an award, success etc. Please contact the parent/guardian and seek approval on a post by post basis

Photographs

● All parents have been sent the updated photography consent agreement, including social media. SIMS keeps a record of all students who do not have consent to have their photos taken and staff will be given an updated list in October 2022

● Staff should check the no photo list before posting any images on social media

● Student names should not appear alongside photographs in external reports or publicity, unless parents have given explicit permission

● The social media checklist must be adhered to and signed before any post is uploaded to a social media platform.

Educational Trips and Residentials

● Images and social media posts about residential visits and school trips must not be uploaded until the children have returned from the event.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Mobile devises should be handed to the class teacher as soon as children arrive at school and will be handed back at the end of the school day. The school does not take responsibility for devises when they are in the possession of members of staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

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

Smart watches are not permitted in school for use by children.

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 by always installing 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 the ICT manager.

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 computing. 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.

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 up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, 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.

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 DSL. At every review, the policy will be shared with the trust board. 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.

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

Early Years and KS1 Acceptable Use and Online Safety Agreement

To stay SAFE online and on devices:

I only USE devices or apps, sites or games if a trusted adult says so and I LOOK AFTER equipment

I ASK for help if I'm stuck or not sure

I TELL a trusted adult if I'm upset, worried, scared or confused

If I get a FUNNY FEELING in my tummy, I talk to an adult

I look out for my FRIENDS and tell someone if they need help

I KNOW people online aren't always who they say they are

I tell a trusted adult if I get a MESSAGE from someone I don't know

Anything I do online can be shared and might stay online FOREVER

I don't keep SECRETS or do DARES AND CHALLENGES just because someone tells me I have to

I don't change CLOTHES in front of a camera

I always check with a trusted adult before SHARING personal information (like my name, address or telephone numbers)

I only use my username and password at school and I don't SHARE my password with anyone

I am KIND and polite to everyone

My name is:

My trusted adults are:

School

Home

Appendix 2

KS2 Acceptable Use and Online Safety Agreement

This agreement will help keep me safe and help me to be fair to others

I learn online – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. School internet and devices are monitored.

I ask permission – Whether at home or school, I only use the devices, apps, sites and games I am allowed to, at the times I am allowed to.

I am a friend online – I won't share anything that I know another person wouldn't want shared, or which might upset them. And if I know a friend is worried or needs help, I will remind them to talk to an adult, or even do it for them.

I am a secure online learner – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!

I am careful what I click on – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes add-ons can cost money, so it is important I always check for these too.

I ask for help if I am scared or worried – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

I know it's not my fault if I see or someone sends me something bad – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.

I communicate and collaborate online – with people I already know and have met in real life or that a trusted adult knows about.

I know new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.

I don't do live videos (livestreams) on my own – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.

I keep my body to myself online – I never get changed in front of a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

I say no online if I need to – I don't have to do something just because a friend dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no and tell a trusted adult immediately.

I tell my parents/carers what I do online – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.

I am private online – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.

I am careful what I share and protect my online reputation – I know anything I do can be shared and might stay online forever (even if I delete it).

My name is: _____

My trusted adults are:

School _____

Home _____

_____

Appendix 3

Latchmere Academy Trust

Acceptable IT Use Statement (staff)

Failure to comply with the requirements of this statement may, at the discretion of Latchmere Academy Trust, result in temporary or permanent loss of access rights. It should be noted that the use of a computer system without permission or for a purpose not agreed by the Trust could constitute a criminal offence under the Computer Misuse Act 1990.

These conditions of use have been drawn up to protect the interests of the Trust, its schools, staff and students. These conditions may be changed at the discretion of Latchmere Academy Trust at any time.

The IT facilities are owned by the Trust and their use is an entitlement for all students, staff and other authorised users subject to the conditions detailed here.

The IT facilities are subject to continual monitoring via software (Securus) which will identify and record all misuse on the Trust's devices, including the identity of the user.

Staff wishing to use the resources must sign a copy of this statement and return it to the Trust. Once approved, access rights will be established. A record will be maintained of all users with system access. Users will be removed from this record when access is no longer required, in accordance with the Data Protection Act. Staff may alternatively confirm the declarations overleaf by responding to the email sent to all staff on 1 September 2022.

Revisions to this statement will be publicised on-screen.

Users may be required to acknowledge their continuing acceptance of the currently prevailing conditions during the logon process.

Conditions:

- All IT-based activity must be appropriate to a school environment.
- Access must be made to the IT resources only via the user's authorised account and password, which must not be made available to any other person. Where necessary, users must be able to produce proof of identity on demand when using ICT resources.
- Activity that threatens the integrity of the Trust's facilities, or activity which corrupts other systems, is forbidden.
- The Trust's policies must be observed at all times, for example: GDPR Privacy notice, online safety and computing.
- The Trust reserves the right to monitor the use of IT resources at any time including examining or deleting any files held on its resources and to monitor both files held and Internet sites visited.

- Use of the Internet to access inappropriate materials is forbidden.

Please note: In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils.

The Trust will take all reasonable precautions to ensure that users access only appropriate material. It is not possible, however, to guarantee that particular types of material will never appear on a terminal, given the international scale and linked nature of information stored on the Internet.

The Trust cannot accept liability for any such material accessed, or any consequences thereof.

- By logging on to the Trust's IT resources users agree to abide by the terms of the Trust's Acceptable IT Use Statement.

- By logging on to the Trust's IT resources users agree not to use them to:

- access chat services, or Internet Relay Chat (IRC) channels or other forms of instant messaging systems (e.g. MSN Messenger) without express permission,

- download inappropriate files / software from the Internet,

- publish information which could identify the user, the Trust or its schools or any other person directly on any Web page,

- send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person, including the reputation of the Trust,

- upload, download or otherwise transmit commercial software or any copyrighted materials,

- introduce any form of computer virus into the network,

- transmit unsolicited commercial or advertising material,

- use this service to set up or run personal businesses,

- send chain letters,

- broadcast unsolicited personal views on social, political or religious matters,

- represent personal opinions as those of the Trust.

User's Full Name ……

User's Signature ……

Date ……

User’s normal place of work (School name)……..

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 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 5

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**