S103/A0124

BANSTEAD

COMMUNITY JUNIOR

SCHOOL

COMPUTING AND ON-LINE SAFETY POLICY

2024

School Resources Committee
Prepared by: Computing Leader/IT Manager
Created/reviewed: January 2024
Date of next review: January 2025

Contents

BANSTEAD COMMUNITY JUNIOR SCHOOL
COMPUTING AND ON-LINE SAFETY POLICY

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- 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 devices')
- 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 child-tochild 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 nonconsensual 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 Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
The governing 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 governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Amy Cooper (Safeguarding governor).

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 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 Safeguarding Team

Details of the school's DSL and backup DSL's are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.
The Safeguarding team in cooperation with the Network Manager take responsibility for online safety in school, in particular:

- Supporting the senior leadership team in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Network manager to make sure the appropriate systems and processes are in place
- Working with the senior leadership team, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged using CPOMS (see appendix 4 for proforma for reporting to gov.) 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 3 contains a self-audit for staff on online safety training needs). This includes promoting staff access and use of the

'National Online Safety' resource (https://nationalonlinesafety.com/)

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually 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 immediately reported to the safeguarding team, reported on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are immediately reported to the safeguarding team and dealt with appropriately in line with the school behaviour policy. Such instances must be logged on CPOMS.

This list is not intended to be exhaustive.

The Network Manager is Robert Holyoake.

3.5 All Staff and Volunteers

All staff, including contractors, 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 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the safeguarding team is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by speaking directly with a member of the safeguarding team and recording the incident on CPOMS.

- Following the correct procedures by speaking with the safeguarding team and Network Manager if they need to bypass the filtering and monitoring systems for

  Educational purposes. A written record of this reason (including the date) will be maintained by the safeguarding team.
- Working with the safeguarding team to ensure that any online safety incidents are logged using CPOMS (see appendix 4 for DSL pro-forma for reporting to gov.) 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 and recorded on CPOMS
- 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

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 (appendix 1)

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
- Hot topics and parent resource sheets / training - National Online Safety

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 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. The information 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 primary schools have to teach:

- Relationships education and health education in primary schools. Pupils 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 (such as PSHE) where relevant.

5. Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters and other communications home (e.g. text, email, weekly whole school newsletter, termly newsletter) as well as in information shared via our website. This policy will also be shared with parents / guardians.

Online safety will also be covered during parents' evenings and an annual child led assembly which parents / guardians are invited to attend.

The school will let parents / guardians 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 / guardians have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher (DSL) and/or class teacher.

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 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. 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, 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 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.

6.3 Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school 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 co-operation

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 staff member in conjunction with 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/guardian 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
- The school behaviour policy / searches and confiscation 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.

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 and restrict access through filtering systems where appropriate.

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

8. Using Mobile Devices in School

Years 5 and 6 pupils may bring mobile devices into school, but they must leave them (switched off) at the school office at the start of the day and collect it again at the end of the school day, making sure that the device remains turned off until they have left the school premises. The school will not accept responsibility for any mobile device brought into school.

Staff personal devices must not be used when children are present unless in an emergency, e.g. during an offsite educational visit.

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 locked when not in use.
- Not sharing the device among family or friends

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 2.

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 senior leadership team and / or the Network Manager.

10. 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 discipline. 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 code of conduct / staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

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, ebulletins 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 safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. With the Network Manager 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.

12. Monitoring Arrangements

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

This policy will be reviewed every year by the safeguarding team in cooperation with the Network Manager. At every review, the policy will be shared with the governing 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.

13. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Discipline Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices

- Complaints procedure
- ICT and Internet Acceptable Use Policy

14. Spiritual, Moral, Social and Cultural Development

Where possible, lessons, either through specific planning or ad-hoc opportunities, will promote the spiritual, moral, social and cultural development of pupils and their understanding of the role of society and their place within it. Through this approach, the school and specific subject teaching, aims to prepare pupils for the opportunities, responsibilities, experiences and challenges of their current and later lives.

15. British Values

The School will ensure in policy and practice that it adheres to the fundamental British Values as detailed in Ofsted Handbook for Inspection, August 2016. The fundamental British Values include valuing democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs. The pupils will be taught to develop and demonstrate skills and attitudes that will allow them to participate fully in and contribute positively to life in modern Britain.

Appendix 1: Pupil Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR PUPILS

Dear Parent/Carer

Computing including the internet, email, and mobile devices is an important part of learning in our school. We expect all children to be safe and responsible when using any computing resources in the school

Please discuss these On-line Safety rules with your child. If you have any concerns please refer to the school website (www.bcjs.org.uk) where there are links to other helpful sites with a wealth of information on this subject.

I will:

- always use the school's ICT systems and the internet responsibly and for educational purposes only.
- only use them when a teacher is present, or with a teacher's permission.
- keep my username and passwords safe and not share these with others.
- keep my private information safe at all times and not give my (or another child's) name, address or telephone number to anyone without the permission of my teacher or parent/guardian.
- tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others.
- make sure that all computing contact with other children and adults is appropriate, responsible, polite and sensible. If someone tries to communicate with me that I do not know, I will immediately inform the teacher.
- be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
- always log off or shut down a computer when I'm finished working on it.

I will not:

- access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity.
- open any attachments in emails, or follow any links in emails, without first checking with a teacher.
- use any inappropriate language when communicating online, including in emails.
- create, link to or post any material that is offensive, obscene or otherwise inappropriate
- log in to the school's network using someone else's details.
- arrange to meet anyone offline without first talking to my parent / guardian / a trusted adult about it.

I know that my use of any school devices can be checked and that my parent/carer contacted if a member of the school staff is concerned about my safety.

I understand that if there is a concern about internet misuse I will speak to my teacher or the headteacher.

Parent/Carer Signature

I/We give permission for our child ……..(child's name) in ……..…(Class) to have access to devices that will have internet access, and that they will follow the On-line safety rules, as set out above, whilst supporting the safe use of Computing at Banstead Community Junior School.

Parents/Carer Signature	**Date:**
……..	…….

Appendix 2: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff, Governors, supply and visitors are aware of their individual responsibilities when using technology. All staff members, Governors, supply and visitors (where applicable) are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher.

Name of staff member / governor / volunteer / visitor (please delete as appropriate):

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will:

- take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
- respect copyright and intellectual property rights.
- ensure that all electronic communications with pupils and other adults are appropriate.
- ensure that personal data (including data held on SIMs systems) is kept secure at all times and is used appropriately in accordance with GDPR legislation.
- ensure that images of pupils and / or adults will be taken, stored and used for professional purposes in line with school policy (see Safeguarding and Child Protection Policy) and with written consent of the parent / guardian.
- report any known misuses of technology, including the unacceptable behaviours of others.
- be an active participant in online safety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
- take responsibility for reading and upholding the standards laid out in the AUP.
- support and promote the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- only use my school email account to send and receive school related emails.

I have a duty to:

- respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.
- report failings in technical safeguards which may become apparent when using the systems and services.
- protect passwords and personal network logins, and should lock or log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users" data, or compromise the privacy of others in any way, using any technology, is unacceptable.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:
AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- use them in any way which could harm the school's reputation.
- be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory / inflammatory comments made on social network sites, forums and chat rooms. I will not add pupils or family members of pupils as 'friends' on any social network site.
- access social networking sites (with the exception of the school X feed).
- use any improper language when communicating online, including in emails or other messaging services.
- install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- share my password with others or log in to the school's network using someone else's details.
- take photographs of pupils without checking with teachers first (applicable to supply / visitors / governors)
- distribute images outside the school network without the prior permission of the parent / guardian, or person/s in the image.
- share confidential information about the school, its pupils or staff, or other members of the community.
- access, modify or share data I am not authorised to access, modify or share.
- promote private businesses, unless that business is directly related to the school.
- use the school system(s) for personal use during working hours.
- use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
- I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and, school emails and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the safeguarding team and Network Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.
- I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.
- I will ensure that all electronic communications with parents, pupils and staff, including email,

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS	
• I have read and agree to follow this agreement alongside the schools Code of Conduct and Policy on the Use of Social Media, to support the safe use of ICT throughout the school.	
Signature of staff member / governor / volunteer / visitor: **(please delete as appropriate)**	**Date:**

Appendix 3: 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?	
Signature of Staff Member / Volunteer	

Appendix 4: 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**