Kingsway Community Primary School

Document Reference Number (if already used)	**2**
Title	Online Safety Policy
Policy Owner	Sara Hartshorn
Version	2.1
Approved Date	18.03.26
Approving Body	School Standards Committee
Next Review Date	March 2027

Version Control

Version	Last Modified	Last Modified By	Document Changes
2.1	March 2026	Sara Hartshorn	Title changed to Online Safety Policy; additional sections included on remote learning, examining electronic devices and use of devices by visitors; child-on-child abuse and sexual harassment included in cyber-bulling section; filtering explicitly included in monitoring section; personal use of social media included in acceptable use section; additional info included re. Cybercrime; explicit reference to monitoring online radicalisation included; SEND specific references included; bullets aligned; page numbers adjusted; section numbers adjusted; key terminology explicitly defined

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, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit others 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

2. 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 considers the National Curriculum Computing programmes of study.

3. Roles and responsibilities

3.1 The School Standards Committee

The School Standards Committee has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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 and that a whole school approach to safeguarding and related policies and/or procedures is implemented
- 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

3.2 The Headteacher

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

3.3 The Designated Safeguarding Leads

Details of the school's designated safeguarding leads (DSLs) are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

DSLs take 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 Child Protection and Safeguarding 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 our school's Behaviour and Relationships 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 School Standards Committee

This list is not intended to be exhaustive.

3.4 The ICT Manager – Savvy IT Ltd

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 three-monthly 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL team 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 our school's Behaviour and Relationships Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff 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/Carers 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/Carer resource sheet – Childnet International

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. All schools must 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:

- 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. The school will also educate pupils on the risks associated with cybercrime, including hacking, Distributed Denial of Service (DDoS) attacks, use of illegal streaming/download sites and bypassing filters.

Where necessary, teaching about safeguarding including online safety will be adapted for

vulnerable children, victims of abuse and some pupils with SEND.

Online safety teaching will also consider the protected characteristics as defined in the Equality Act 2010, ensuring children know how to report discrimination.

5. Educating parents/carers about online safety

The school will raise parent/carer awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

The school will let parents/carers 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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with a DSL.

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

6. *Child-on-child abuse* including *cyber-bullying* and *sexual harassment*

Kingsway Community Primary School treats online child-on-child abuse with the same seriousness as offline abuse.

6.1 Definitions

Child-on-child abuse refers to abusive behaviour by one child that harms another child, including physical, sexual, emotional abuse, exploitation, bullying, coercive control, harassment, or harmful behaviour occurring either in person or online.

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 Kingsway's Behaviour and Relationships Policy)

Sexual harassment is unwanted behaviour of a sexual nature that violates someone's dignity or creates an intimidating, hostile, degrading, humiliating or offensive environment, regardless of intent. This can also be in person or online.

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 tutor groups.

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 10 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, Kingsway will follow the processes set out in our school's Behaviour and Relationships 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.

A DSL will report the incident and provide the relevant material to the police as soon as it 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 Online sexual harassment

Online sexual harassment encompasses misogynistic content, upskirting, unwanted sexual images and non-consensual sharing of images, amongst other things.

All staff, governors and volunteers (where appropriate) receive training on sexual harassment, including online, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of online sexual harassment, Kingsway will follow the processes set out in our school's Behaviour and Relationships 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.

A 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.

7. Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, 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, the authorised staff member will:

- Assess how urgent the search is, and consider the risk to other pupils and staff

- 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

When they believe there is a good reason to do so, the authorised staff members may ask a parent/carer to support them in examining, and if necessary, erase any data or files from an electronic device that they have confiscated.

Authorised staff members will not examine data or files on an electronic device unless a parent/carer is present and only if the staff member reasonably suspects 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 a staff member believes that there may be inappropriate material on the device, they must not, under any circumstances, view this material. It is up to the Headteacher, in conjunction with SLT and DSLs, to decide on a suitable response. If there are believed to be 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 ask parents/carers to delete it if they reasonably suspect that its continued existence is likely to cause harm to any person.

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

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

8. Acceptable use of the internet in school and personal use of social media

8.1. Acceptable Use Agreements

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). As part of this agreement, it is made clear that staff/volunteers/governors may only have parents/carers added on social media under the following circumstances:

- This is part of a genuine friendship/social contact which is independent of the professional relationship e.g. part of the same family/personal network or social recreational circle. Members of staff/volunteers/governors should not establish or seek to establish social contact with pupils or their families for the purpose of securing a friendship or to pursue or strengthen a relationship.
- This is openly acknowledged and explicitly declared in writing by staff/volunteer to the Headteacher. Governors would need to declare this to the Chair of Governors; the Chair of Governors would declare this to the Clerk of the School Standards Committee.
- Care is always taken by the member of staff/volunteer/governor to maintain appropriate personal and professional boundaries in these circumstances.

The agreement also states that online contact with pupils is explicitly prohibited except through the identified, approved channels.

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.

8.2 Staff/Volunteers/Governors Personal Use of Social Media

Staff/Volunteers/Governors are expected to maintain professional standards of behaviour when using social media and online platforms, including in their personal time.

Personal social media accounts should not be used to:

- communicate with pupils or former pupils

- send or accept friend requests or follow requests from pupils

- discuss confidential school matters or individuals connected with the school

Staff/Volunteers/Governors are advised to:

- set the highest possible privacy settings on personal accounts

- avoid posting content that could bring themselves or the school into disrepute

- assume that anything shared online may become public, regardless of privacy settings

Staff/Volunteers/Governors must not:

- use personal accounts for school-related communication

- share images of pupils or identify pupils, parents/carers or colleagues online

- engage in online behaviour which could be interpreted as grooming, harassment, or inappropriate conduct

Any concerns regarding staff online conduct that may pose a safeguarding risk must be reported to the Designated Safeguarding Lead (DSL) and will be managed in line with Kingsway's Child Protection and Safeguarding and Code of Conduct policies.

8.3 Ongoing monitoring of internet use

Kingsway Community Primary School 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 and is linked to the Code of Conduct Policy.

9. Pupils using mobile devices in school

Year 6 pupils may bring mobile devices into school, but are not permitted to use them on site during the school day including:

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

All mobile phones must be handed in to the school office for safekeeping for the duration of the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with our school's Behaviour and Relationships Policy, which may result in the confiscation of their device.

10. 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 using strong passwords or passphrases
- 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 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 Savvy IT.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in

accordance with the staff disciplinary procedures/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.

12. Use of devices by visitors

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Visitor access to the internet is limited to 'Guest Wi-Fi.'

13. 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 harm*** such as 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).

This training also covers the differences between ***safeguarding*** and ***child protection***.

13.1 Terminology

Safeguarding and promoting the welfare of children refers to the process of providing help and support to meet the needs of children as soon as problems emerge; protecting children from maltreatment, whether that is within or outside the home, including online; preventing the impairment of children's mental and physical health or development, ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.

Child protection refers to the actions taken when there is a concern that a child is suffering, or is likely to suffer, significant harm.

Online harm refers to any negative or damaging experience that a child may encounter through the use of digital technologies, the internet or online services, which impacts their safety, wellbeing or development.

Sexting, also referred to as ***sharing nudes***, is the creation, sharing or possession of an image, video or message of a sexual nature, including partially nude or nude images, using digital technology. Involving children under the age of 18 in such images is always a safeguarding issue and may be illegal, even if the content is shared consensually.

13.2. Content of training

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
    - ***Sexting***, including 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 DSLs 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 related to 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.

14. Remote Learning

On the rare occasion when remote learning is necessary, the following points will apply:

- school approved platforms will be used for online learning (e.g. Studybugs, Zoom, Microsoft Teams)
- school staff will retain full control of the platform
- pupil cameras and microphones will be disabled/muted
- pupils will not be able to share screens
- live lessons will not be recorded
- clear expectations will be given to pupils and parents outlining expectations e.g. that links to meetings must not be shared by participants, parents should stay in audible proximity
- DSLs will oversee online safety considerations where necessary
- full risk assessments will be completed before remote teaching begins

This section links to the Kingsway Community Primary School Remote Learning Policy and is underpinned by the Child Protection and Safeguarding Policy.

15. Filtering and Monitoring arrangements

The DSL is responsible for filtering and monitoring at Kingsway Community Primary School. The link Governor for Safeguarding is responsible for checking this. Staff are trained annually in expectations regarding ***filtering*** and ***monitoring***.

15.1 Terminology

Filtering refers to the technical systems and processes used by a school to restrict access to inappropriate, harmful or illegal online content when using the school's internet, networks and devices.

Monitoring refers to the processes used by a school to observe, review and respond to how digital technology and online services are used on school networks and devices, to identify potential safeguarding or online safety concerns.

15.2 Kingsway's Specific Filtering and Monitoring arrangements

Kingsway uses Smoothwall as its filtering system. Smoothwall is compliant with the Department for Education's (DfE) Broadband internet standards for schools and colleges, ensuring that it provides appropriate protection from inappropriate content and meets the filtering part of the DfE Filtering and Monitoring Standards.

The effectiveness of this system is tested every 6 weeks by the IT Manager and outcomes recorded and shared with the DSL. These checks form part of the formal annual review recommended by the DfE.

This filtering does not unreasonably impact on teaching and learning. When filtering blocks legitimate sites, the IT Manager investigates this and rectifies the issue straight away.

Warwickshire Digital Safeguarding Team inform the DSL at Kingsway if there are any concerns following online searches on school devices. This meets the monitoring part of the DfE Filtering and Monitoring Standards. These alerts are in real time, and either email or phone based, dependent on the level of concern. They are based on key words or searches on all devices including remote or mobile. The DSL then takes necessary action, recording this on My Concern.

This also includes the flagging of risky content related to the monitoring of online radicalisation as part of the Prevent Duty. A DSL would respond to this online activity immediately, taking proportionate action to assess and address any potential risk which would include reviewing the concerning online behaviour, contextual information and any associated patterns. The DSL would then follow safeguarding procedures and statutory guidance, working closely with external safeguarding partners, including the local Prevent team or police where appropriate.

A DSL logs all behaviour and safeguarding issues related to online safety, ensuring ongoing monitoring and support for the pupil(s) as needed. An incident report log can be found in Appendix 5 and is linked to the Child Protection and Safeguarding Policy.

16. Policy Review and links with other policies

16.1 Policy review

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the governing board. This is important because technology, and the risks and harm related to it, evolve and change rapidly.

16.2 Links with other policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour and Relationships Policy
- Disciplinary Policy
- Data Protection Policy and privacy notices
- Complaints procedure
- Acceptable Use policy
- Remote Learning Policy
- Code of Conduct Policy

Appendix 1: EYFS/KS1 Acceptable Use Agreement for pupils and parents/carers

ACCEPTABLE USE OF KINGSWAY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

This agreement is to help stakeholders promote and establish safe and responsible working practices in accordance with Kingsway's Online Safety Policy.

Name of pupil:	**Date of birth:**

When I use the Kingsway's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or another trusted adult if I can do so before using them
- Only use websites that a teacher or other trusted adult has told me or allowed me to use
- Tell my teacher or other trusted adult immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
- Use school computers for schoolwork only
- Be kind to others and not upset or be rude to them
- Look after Kingsway's ICT equipment and tell a teacher or other trusted adult straight away if something is broken or not working properly
- Only use my own username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone number) to anyone without the permission of my teacher, other trusted adult or parent/carer
- Save my work on the school network
- Check with my teacher or other trusted adult before I print anything
- Log off or shut down a computer when I have finished using it

I agree that Kingsway Community Primary School will monitor the websites I visit to help keep me safe.

Signed (pupil):	**Date:**

Parent/Carer agreement:
I agree that my child can use Kingsway's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

I will make sure my child understands these rules and talk to them about staying safe when using technology.

Signed (Parent/Carer):	**Date:**

Appendix 2: KS2 Acceptable Use Agreement for pupils and parents/carers

ACCEPTABLE USE OF KINGSWAY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

This agreement is to help stakeholders promote and establish safe and responsible working practices in accordance with the school Online Safety Policy.

Name of pupil:	**Date of birth:**

I will read and follow the rules in this acceptable use agreement.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher or another trusted adult is present, or with their permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher, other trusted adult or parent/carer
- Tell a teacher (or other trusted adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher or other trusted adult 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, upsetting, inappropriate or unsafe
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, unstructured time, clubs or other activities organised by the school and will hand it in to the school office for safekeeping for the duration of the school day.

I agree that the school will monitor the websites I visit to help keep me safe.

Signed (pupil):	**Date:**

Parent/Carer's agreement:
I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff.

I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.

I will make sure my child understands these rules and talk to them about staying safe when using technology.

Signed (Parent/Carer):	**Date:**

Appendix 3: Acceptable Use Agreement for staff, governors, volunteers and visitors

ACCEPTABLE USE OF KINGSWAY'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS This agreement is to help stakeholders promote and establish safe and responsible working practices in accordance with the school Online Safety Policy.
Name of staff member/governor/volunteer/visitor:
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 • Access social networking sites or chat rooms for personal use during working time or in a way that breaches professional standards • 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 or videos of pupils without appropriate permission and authorisation being in place • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school • Engage in unprofessional behaviour when using personal social media or online platforms, including adding parents/carers except where this forms part of a genuine friendship independent of the professional relationship • Have online contact with pupils apart from as part of the school identified, approved channels
I understand that I am responsible for the safe and appropriate use of any school-issued device or account and must report any loss, theft, damage or suspected data breach immediately in line with the school's procedures. I understand that I must only use the school's ICT systems, internet access and email accounts for educational purposes and/or to fulfil the duties of my role. I understand that the school uses appropriate filtering and monitoring systems on its ICT networks and devices to support safeguarding and the safety and wellbeing of pupils and staff, and that monitoring is carried out proportionately and in line with data protection legislation. I will take all reasonable steps to ensure that work devices and any personal devices used to access school data are secure and password protected, and that all school data is stored and handled in accordance with the school's Data Protection Policy, including the use of encryption where required. I will inform the Designated Safeguarding Lead (DSL) and ICT Manager (Savvy IT) if I encounter, or am made aware of, online material that may upset, distress or harm pupils or others. I will use the school's ICT systems and internet responsibly, ensure that pupils in my care do so, and follow the school's expectations regarding the use of mobile phones and personal devices. I understand that failure to follow this agreement or the school's Online Safety Policy may be addressed in line with the school's policies and procedures.
Signed (staff member/governor/volunteer/visitor): | **Date:**

Appendix 4: Example 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 to access 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: Example 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**

16