Online Safety and Acceptable Use Policy

Approved by Grove House Nursery School Full Governing Body	**Approval Date**	September 2026
	Review Date	September 2027

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 6
5. Educating parents/carers about online safety 6
6. Cyber-bullying 6
7. Acceptable use of the internet in school 7
8. Photography and videography 7
9. Staff using work devices outside school 8
10. How the school will respond to issues of misuse 8
11. Training for staff, governors and volunteers 8
12. Monitoring arrangements 9
13. Links with other policies 9
Appendix 1: Visitor Agreement 11
Appendix 2: acceptable use agreement (staff, governors, volunteers, students and visitors) 12
Appendix 3: online safety incident report log 14

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 families 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 phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – 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), including those generated using AI, and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

2. Legislation and guidance

This policy is based on the statutory safeguarding guidance, Keeping Children Safe in Education from the Department for Education (DfE) and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying
- Searching, screening and confiscation
- Mobile phones in schools

It also refers to the DfE's guidance on protecting children from radicalisation and the Early Years Foundation Stage Statutory Framework.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Children's Wellbeing and Schools Act 2026 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.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing body will ensure online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement.

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

The governing body will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing body will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and that a review of the effectiveness of the filtering and monitoring systems is carried out by SLT at least once every academic year. The governing body will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the 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 the school's safeguarding needs

All governors will:

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Make sure 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 2)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure 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 making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

They will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies 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 making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing body to review this policy every 3 years and make sure 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- 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's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Making sure 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
- 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
- Undertaking annual risk assessments that consider and reflect the risks pupils 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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

This list is not intended to be exhaustive.

3.4 The Senior Leadership Team (SLT)

The SLT are 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Knowing that the DSL 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 informing the DSL without delay, or contacting Grove House Nursery Schools IT support provider, Trusol - 03456 121222, in the event that the DSL is unavailable.
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this 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'
- Understand and adhere to Grove House Nursery School's mobile phone procedures as detail in our safeguarding and child protection policy

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Understand and adhere to Grove House Nursery School's mobile phone procedures as detail in our safeguarding and child protection policy

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

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 and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Visitors and members of the community will also be expected to understand and adhere to Grove House Nursery School's mobile phone procedures as detail in our safeguarding and child protection policy

4. Educating pupils about online safety

Pupils will be supported to develop the foundations of online safety

At Grove House Nursery School, children are at the earliest stages of learning about technology and the digital world. Through adult-led activities, conversations, stories and supervised use of technology, children will be supported to develop age-appropriate awareness of staying safe, including:

- Learning that technology should be used safely and with adult support.
- Beginning to understand that some information is private and should not be shared.
- Knowing that they should tell a trusted adult if something they see, hear or experience makes them feel worried, upset or confused.
- Developing positive habits for using technology in a safe, healthy and balanced way.

Online safety messages will be embedded throughout the curriculum and adapted to meet the developmental needs of individual children, including those with SEND and other vulnerabilities.

5. Educating parents/carers about online safety

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

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

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

6. Cyber-bullying

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.

Due to the age of the children attending the nursery, cyber-bullying between children is unlikely to be a significant concern within the setting. However, staff should remain alert to any information or concerns that suggest a child may be affected by cyber-bullying, online harassment or harmful online behaviour within their family or wider community.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Any such concerns must be reported to the Designated Safeguarding Lead (DSL) without delay and managed in line with the nursery's safeguarding and child protection procedures.

7. Acceptable use of the internet in school

All staff, volunteers, students 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

8. Photography and videography

At Grove House Nursery School, we recognise that photographs and videos are a valuable part of children's learning and development. They enable us to document children's achievements, support assessment and planning, celebrate progress, create engaging displays, and share learning experiences with children and their families.

Images and recordings help us to capture important moments in children's learning journeys and provide meaningful opportunities for reflection, discussion and communication between nursery and home. We are committed to using photography and videography in a way that is professional, purposeful and centred on the best interests of each child.

We use images and videos safely by:

- Obtaining informed consent from parents/carers before taking, storing or using images and videos of children, and ensuring that all use of images is in line with the permissions provided.
- Maintaining accurate records of parental consent and reviewing these regularly to ensure they remain current.
- Using photographs and videos only for legitimate educational and nursery purposes, including assessment, learning journeys, displays, staff training, celebrating children's achievements and sharing learning with families.
- Sharing photographs and videos with parents/carers only through approved nursery systems, such as the Ovivo app, or other authorised methods approved by the nursery.
- Ensuring that all images and videos are taken and stored only on nursery-owned devices and systems.
- Prohibiting the use of personal mobile phones, cameras, tablets, smart watches or any other personal devices to take, store, transmit or share images or videos of children.
- Storing all images and videos securely and restricting access to authorised staff members who require access for their professional role.
- Taking images in a manner that preserves children's dignity and respects their privacy at all times.
- Carefully considering the content of photographs and videos to ensure that children are appropriately clothed and that images cannot be misused or misinterpreted.
- Ensuring that images and videos are not copied, downloaded, shared or transferred outside approved nursery systems unless specifically authorised and required for a legitimate nursery purpose.
- Removing or securely deleting images and videos when they are no longer required, in accordance with the nursery's data retention procedures.

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Providing staff with clear guidance and training on the safe and appropriate use of photography and videography.
- Reporting any concerns regarding the misuse, loss, unauthorised sharing or inappropriate use of images immediately to the Designated Safeguarding Lead (DSL) and Headteacher.
- Complying with all relevant safeguarding, data protection and confidentiality requirements when taking, storing, using and sharing images and videos.

To protect the privacy and safety of all children, parents, carers and visitors are not permitted to take photographs or videos whilst on nursery premises.

All visitors are required to sign in at the main office on arrival. As part of this process, visitors will be asked to hand in any mobile phones or devices capable of taking photographs or videos and to sign an agreement confirming that they will not take, record, store or share images of children, families or staff whilst on site. Further details can be found in the nursery's safeguarding and child protection policy. See appendix 1.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected, and updating passwords every 3 months – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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
- Never sharing the device among family or friends
- Each device must have appropriate anti-virus and anti-spyware protection installed and maintained by the nursery's ICT service provider. If a device displays any security warnings, virus alerts or other concerns relating to its protective software, staff must immediately stop using the device and report the issue. The device must not be used again until it has been inspected and confirmed as safe by the ICT service provider.
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that 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 Trusol, the school's ICT service provider. Staff must also inform a member of the senior leadership team about any concerns.

10. How the school will respond to issues of misuse

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 and disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. Training for staff, governors and volunteers

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

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, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, including images generated or altered by AI, especially around chat groups
- Sharing of abusive images and pornography, including images generated or altered by AI, 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 and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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 safeguarding and child protection policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every 3 years by the headteacher. At every review, the policy will be shared with the governing body. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks relating to online safety. 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:

- Safeguarding and child protection policy
- Staff code of conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

- Complaints and compliments policy
- Data retention procedures

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 1: Visitor Agreement

Visitor Signing in Sheet	Date:

To help safeguard children and protect their privacy, I understand and agree that:

I have left my mobile phone and any other personal recording devices in the school office for the duration of my visit.

I will not use a mobile phone, smart watch, tablet, camera, or any other device capable of taking photographs, recording video, or recording audio while on the school site.

I will follow all school safeguarding procedures and instructions given by staff during my visit.

If I need to access my phone in an emergency, I will seek permission from a member of staff and return to the school office.

By signing in below I agree that I have read, understood and agreed to adhere to the declaration above.

Name	Time In	Phone In (signed)	Staff Initials	Phone Out (signed)	Staff Initials	Time Out

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 2: acceptable use agreement (staff, governors, volunteers, students and visitors)

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

AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS, STUDENTS AND VISITORS

Name of staff member/governor/volunteer/student/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 that could harm the school's reputation
- Access social networking sites or chat rooms
- 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
- Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils or within the nursery school on any personal devices
- 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
- Discuss school issues on social networking sites.
- Give out to children or their parents or family, my own personal contact details, such as mobile phone number, personal social networking details and personal email address

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS, STUDENTS AND VISITORS	
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 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 designated safeguarding lead (DSL) know if a pupil informs me they have found any material that 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 will use generative AI in line with the school's online safety and acceptable use policy. I will ensure that all electronic communications with pupils, parents and staff are compatible with my professional role, and never via personal email / phone accounts / social networking profiles. Images & videos of pupils and/or staff will only be taken, stored on school/centre equipment and will only be used for professional purposes in line with school/centre policy and with written consent of the parent, carer or staff member. I will only use my personal mobile phone or other personal electronic devices in designated areas, such as the staff room or outside the nursery's main gates.	
Signed (staff member/governor/volunteer/student/visitor):	**Date:**

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Appendix 3: 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**

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms