Online Safety Policy

Overley Hall School

Approved by:	Support & Scrutiny Board
Last reviewed on:	25 August 2023
Next review due:	6th September 2024

Contents

Aims

At Overley Hall School, we take online safety very seriously and recognise it is our duty to keep the children and young people in our school safe whilst using technology.

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

The 4 key categories of risk

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

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

Legislation

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.

This policy complies with our funding agreement.

Role & responsibilities

The Support and Scrutiny Board (SAS Board)

The SAS Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

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

The SAS Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The SAS 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.

All SAS Board members will:

- Ensure 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

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is individualised for our pupils. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. **Beverley Doran** will take ultimate responsibility for safeguarding and child protection, online safety and understanding the filtering and monitoring systems and processes in place at our setting, in her role as the DSL and as an appropriate **senior member** of staff from our **leadership team**. The responsibility for Online Safety has been delegated to Deputy DSL Lorna Deakin who is also a senior member of staff from our leadership team.

The designated safeguarding lead and deputies

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 ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and SAS 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 Start Technology to make sure the appropriate systems and processes are in place
- Working with the headteacher, Start Technology 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
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and SAS 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.

Start Technology

The Start Technology 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 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 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 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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 completing a concern's/ sensitive information form
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy

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 resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Current protection

K9 web protection – monitors usage
Web Titan – blocks anything deemed inappropriate
ESET – defence against viruses and potential threats
Police Patrol mail security – spam email and harmful attachments filter
Staff and learners have individual computer login accounts
No applications to be downloaded unless by Start Technology
Personal accounts of sites such as Amazon and Netflix should not be used.

Educating learners about online safety.

Pupils will be taught about online safety as part of the curriculum:
All schools have to teach:

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

At Overley Hall School content in relation to Online Safety is delivered in a personalised way according to the young person's level of development.

Examples from the RSE banded Curriculum are:
Blue band – Explore the fact that there maybe people online who do not have our best interests at heart.
Green band - Explain what is meant by hurtful behaviour and bullying (including verbal, physical and emotional for example omission/exclusion/peer pressure, peer influence and online)
Gold band (in greater depth) Identify trusted adults/services that can help us if we or someone we know has been the target of unkind, hurtful, abusive or bullying behaviour, including online.
Cyan (in greater depth) - Identify some strategies, game apps or advertising might use to encourage online gambling and chance based purchases (loot boxes).

The safe use of social media and the internet is also covered in other subjects where relevant and in targeted Theme Days.

Educating parents about online safety.

The school will raise parents/carers' 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.

Online safety will also be covered during parents' evenings.
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 the headteacher.

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

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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy for further details.)

Preventing and addressing cyber-bullying

Due to the profile of learners at Overley Hall School there is a low risk of them being instigators of cyber-bullying but they maybe the victim. High staffing ratio's where all learners are 1:1 aims to reduce the risk of this occurring.

To help learners who are able to use such technology without direct supervision prevent cyber-bullying, we will ensure that they understand what cyber-bullying 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 developmentally appropriate pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Where appropriate 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.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and 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, 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 tutor/teacher or DSL

- 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 DSL 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/carer refuses to delete the material themselves

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

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

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

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

Acceptable use of the internet in school

All learners, parents/carers, staff, volunteers and SAS Board members are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendices 1 and 2). 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, Board members and visitors (where relevant) to ensure they comply with the above.

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

. Pupils using mobile devices in school

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

- Lessons

Staff using work devices outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keeping operating systems up to date by always 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 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 Start Technology.

How the school will respond to issues of misuse

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

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

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

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL 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 child protection and safeguarding policy.

Provision of remote education during Pandemics (e.g. COVID-19).

Due to the nature of Overley Hall School and the profile of its learners it is unlikely that the school will be closed. In the event of the school being closed or a learner needing to 'self-isolate' appropriate work will be provided. If the pupil is resident at Wellingtonia Children's Home the safety measures regarding internet access and supervision will remain the same (the same server is used). If virtual content is part of the curriculum offer, guidance from Safeguarding and remote education during coronavirus (COVID-19) will be used.

Monitoring

The DSL and staff log behaviour and safeguarding issues related to online safety.
This policy will be reviewed on an annual basis unless new government guidance affects its validity.

This policy will be reviewed every year. At every review, the policy will be shared with the SAS board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies.

Safeguarding and Child Protection

Anti-bullying

Behaviour Policy

Prevent Duty

Data protection

Staff Code of Conduct

Complaints Procedure

Personal Mobile Phone and Bring Your Own Device (BYOD) Policy

Blog and Social Networking Policy and Procedures

Appendix 1.

Acceptable Use Agreement.

- I will only use Overley Halls' digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the senior leadership team.
- I will escalate any concerns regarding learners being exploited or abused online immediately to a DSL such as the Headteacher
- I will not reveal my password(s) to anyone or not log on for another to use.
- I will not allow unauthorised individuals to access: E-mail / Internet / Intranet / Network / BehaviourWatch.
- I will ensure all documents, data, etc., are saved, accessed and deleted in accordance with Overley Hall's network, data security and confidentiality protocols.
- At any time I will not use Overley Hall's equipment to browse, download or send material that could be considered offensive or inappropriate to colleagues or learners.
- I will report any accidental access, or receipt of inappropriate materials, or filtering breach to one of the senior leadership team members.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.

- I will not connect a computer, laptop or other device (including USB flash drives), to the network/internet that does not have up-to-date anti-virus software and will keep any ‘loaned’ equipment up-to-date, using Overley Hall’s recommended anti-virus, firewall or other ICT ‘defence’ systems.
- I will not use personally owned camera phones for taking and transferring images of learners or staff and recognise that only in special circumstances, such as emergency situations would a phone be used for such purposes, providing senior leadership permission has been received.
- I will ensure that any private social networking sites or blogs are not used to comment or discuss information relating to the Overley Hall or work colleagues (this includes being aware of personal information posted by others which may bring their conduct into question).
- I will not use personal e-mail addresses, instant messaging identities, social networking accounts for company communication.
- I will not use personal home/mobile telephone numbers for contacting parents or carers.
- I will only use approved and secure e-mail or other approved communication systems, with learners or parents/carers for appropriate ‘work’ business purposes.
- I will not access social media at work or on company computers or phones.
- I understand that there is a difference between my professional and personal life and will therefore not engage in any online activity that may compromise my professional responsibilities. This refers to social networking sites such as Facebook, Instagram or Twitter.
- I agree and accept that any computer, laptop or iPad loaned to me by Overley Hall, is provided solely to support my professional responsibility’s and that I will notify the senior leadership team if a reasonable amount of personal use outside working hours become ‘significant personal use’ as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport form one location to another is protected by encryption and that I will follow Overley Hall’s data security protocols when using such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or learner information, held within Overley Hall’s information management system, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

- I will embed Overley Hall's Online-Safety policy into my working day practice.
- I understand that all Internet or network usage at Overley Hall is monitored and data could be made available to the senior leadership team on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

I (name) ..... agree to abide by this Online-Safety Policy and
Acceptable Usage Policy.

Signature_____Date
_____.....