Glendower Preparatory School

E-Safety Policy

September 2021

Reviewed: September 2021

Next Review: July 2024

Glendower Preparatory School acknowledges the assistance provided by guidance documents prepared by the following public bodies:

The Department for Education (DfE)
The Independent Schools Inspectorate (ISI)

First Created: September 2018

Reviewed: September 2021 (Shoaib Mastan)

Next Review: July 2024

Staff Responsible: Mrs Nina Kingsmill Moore (Headmistress)
Miss Laura Rodgers (Deputy Head Academic)
Mrs Donna Sweeney (Deputy Head Pastoral)
Mr Dominic Tucker (Head of Lower School)
Mr Shoaib Mastan (Head of Digital Learning)
Mr Floyd Ball (ICT Network Manager)

Responsibility for Review: Mr Shoaib Mastan (Head of Digital Learning)

This policy also applies to Early Years Foundation Stage.

Policies and Documents referred to:

- Acceptable Use of ICT Policy
- Taking, Storing and Using Images of Children Policy
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Data Protection Policy
- Glendower Staff Handbook

Contents

1. Introduction

The aim of this policy is to:

- To put in place procedures 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Our approach to online safety includes (but is not limited to) addressing the following categories of risk:

- Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, homophobia, self-harm, suicide, anti-Semitism, 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.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a good reason to do so.

The policy also takes into account the National Curriculum computing programmes of study for computing and PSHE.

2. Roles and Responsibilities

Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Deputy Head Pastoral/Designated Safeguarding Lead (DSL). The governor who oversees online safety is Juliet Richards.

Senior Leadership Team & Head of Digital Learning

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

The DSL alongside the Head of Digital Learning takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT Manager/Network Engineer and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with the Acceptable Use of ICT policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour and anti-bullying policies.
- 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.

IT Manager/Network Engineer

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 regular basis.

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Teaching and Support Staff

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 as outlined in the Acceptable Use of ICT policy, and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour and anti-bullying policies.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).

Parents can seek further guidance on keeping children safe online from the following organisations and websites that will be sent out to them via email or through annual e-safety talks at school.

3. E-Safety in the Curriculum

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

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 their time at the school, we intend for pupils to know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content, and contact and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- Appropriate boundaries 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 majority of the e-safety curriculum will be taught in computing and PSHE lessons. Each academic year, a half-term will be dedicated to an e-safety unit and the school's PSHE scheme of work addresses e-safety issues within it throughout the year. Teachers are expected to incorporate e-safety across all subjects where deemed appropriate, particularly in Year Four and above, as pupils have dedicated access to their own iPads and Microsoft 365 (**MS365**) accounts.

The Head of Digital Learning is responsible for ensuring that pupils are made aware of the rules of using the iPads and the associated consequences should the rules not be followed. The ICT Manager/Network Engineer will work alongside the Head of Digital Learning to ensure that monitoring software is in place to enforce safe usage of the iPads. Software is in place to ensure that any staff member may use their iPad to lock a pupil's iPad should they notice any misuse on the part of a pupil.

Mobile devices are not permitted at school. Year Six may bring mobile phones to school if they travel in to school on their own and these must be handed in to the school office upon arrival and collected at the end of the school day.

In addition, the above members of staff, alongside the Deputy Head Pastoral/DSL, are responsible for monitoring messages sent over MS365 (via Teams or e-mail) to ensure there are no incidents of cyber-bullying taking place. Smoothwall is the school's software that will be used to assist with this and the ICT Manager/Network Engineer is responsible for ensuring that this software is working correctly.

4. Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one

person or group by another person or group, where the relationship involves an imbalance of power. Please refer also to the school's behaviour and anti-bullying policies.

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, the school will ensure that pupils understand the importance of being kind online and thinking before sending any type of message over a device. As part of the e-safety curriculum, they will learn what cyber-bullying is and what to do if they become aware of it happening to themselves or others. The school 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. Form teachers will discuss cyber-bullying with their classes in PSHE lessons and circle time, and it will be taught discretely in computing lessons as well. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

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 via email on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and anti-bullying policies. 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 consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Examining Electronic Devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a good reason to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to cause harm, disrupt teaching, and/or break any school rules. If inappropriate material is found on a device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline), and/or report it to the police.

Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element. Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation

Please also refer to the 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.

5. Training

All new staff members will be required to read this policy and the Acceptable Use of ICT policy as part of their induction. 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 to develop:

- Better awareness to assist in spotting the signs and symptoms of online abuse.
- The ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- 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. 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.

6. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix of this policy. This policy will be reviewed regularly by the Head of Digital Learning. At every review, the policy will be shared with the governing board. Although the date of review is every three years, the policy may be changed at more regular

intervals due to the rapidly changing nature of technology and the risks and harms related to it.

Appendix 1:

Glendower Preparatory School

Acceptable Use Agreement (Upper School)

ACCEPTABLE USE AGREEMENT FOR SCHOOL DEVICES – UPPER SCHOOL	
Name:	
When I use the school's computers and iPads and am on the internet in school I will: • Use the school's devices and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my personal information safe at all times and not give my name, address or telephone number to anyone • Tell a teacher (or other adult who works at the school) immediately if I find any material which might upset me or others • Always log off or shut down a computer when I'm finished working on it • Always lock an iPad and put it back in the charging station when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking websites, chat websites and gaming websites • Open any attachments in emails or Teams, or click on any links, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails or Teams • Log in to the school's devices or online platforms using someone else's details **I understand that the school can monitor the websites I visit and the locations that I have logged in from. I understand that there will be consequences if I don't follow the rules.**	
Signed:	**Date:**

Appendix 2:

Glendower Preparatory School

Acceptable Use Agreement (Lower School)

ACCEPTABLE USE AGREEMENT FOR SCHOOL DEVICES – LOWER SCHOOL	
Name:	
Rules when I use a school computer or iPad: • I will only use them if asked by an adult • I will only use websites that a teacher or adult allowed me to use • I will tell my teacher immediately if I click on a website by mistake • I will tell my teacher immediately if I receive messages from people I don't know • I will tell my teacher immediately if I see anything upsetting on the screen • I will only use the devices for schoolwork • I will look after the school devices and tell a teacher if something is broken • I will only use my own username and password to log in • I will never give my personal information to anyone on the internet **The school checks all the websites that I visit. If I don't follow the rules, I may not be allowed to use school devices again.**	
Signed (pupil):	**Date:**

Appendix 3:

Glendower Preparatory School

Acceptable Use Agreement (Staff/Governors/Visitors)

ACCEPTABLE USE AGREEMENT FOR SCHOOL DEVICES – STAFF/GOVERNORS/VISITORS	
Name:	
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 • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • 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	
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) and Head of Digital Learning know if a pupil informs me that they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed:	**Date:**

Appendix 4:

Glendower Preparatory School

E-Safety Incident Report Form

Report created by	
Name	
Title	
Date	
Staff informed (give name and date)	
Headmistress	
Head of DL	
Network Engineer	
Designated Safeguarding Lead (must be informed in the event of a safeguarding concern)	
Other (give details)	
Nature of concern (give details of the event including the time, date and location and the devices on which the incident occurred)	
Time and date the incident was logged	

Appendix 5:

Glendower Preparatory School

E-Safety Incident Log

Details of all e-safety incidents are to be recorded by the member of staff involved on this Incident Log. The report form should be passed on to the Headmistress, the Head of Digital Learning, and the Designated Safeguarding Lead if there is a child protection concern. Incidents involving cyberbullying also need to be recorded in the Anti-Bullying Log and on iSAMS.

Date/time:
Name of pupil / staff involved
Room and computer / device details
Details of incident (including evidence)
Actions / reasons / consequences