Glendower Preparatory School

Acceptable Use of ICT Policy

January 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)

Reviewed: January 2024

Next Review: January 2025

Staff Responsible: Mrs Nina Kingsmill Moore (Headmistress)
Miss Laura Rodgers (Deputy Head Academic)
Mrs Kemi Ehilebo (Deputy Head Pastoral)
Ms Nuren Parpia (Head of IT and STEM) Ms Jessica Hirani (from Jan 24)
Mx Phoebe Curran (IT Technician)

Responsibility for Review: Ms Nuren Parpia (Head of IT and STEM)/ Ms Jessica Hirani (from Jan 23)

This policy also relates to Early Years Foundation Stage.

Policies and Documents referred to:

- E-Safety Policy
- Images of Children Policy
- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Data Protection Policy
- Glendower Staff Handbook

Contents

1. Introduction

Technology allows access to open worldwide communication, available to everyone at all times. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people.

The aim of this policy is to:

- Ensure that Glendower Preparatory School (**the school**) complies with its obligations under the Data Protection Act 2018 (**the Act**). This policy is aimed at all staff including temporary staff, agency workers, volunteers and all other people when working in or for the school (whether directly or indirectly) and applies to Governors.
- Protect the good reputation of the school and support and enable effective use of technology.
- Set out the key principles expected of all members of the school community with respect to the use of ICT. Whilst most of this policy relates to the use of ICT, Section 4 (Information Security) also deals with information held in paper / hard copy.
- Safeguard and protect the children and staff of the school.
- Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal, or recreational use.
- Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other School policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

This policy applies to all members of the school community (including staff, pupils, parents, visitors) who have access to and are users of school ICT systems, both in and out of the school. The school will deal with e-safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, including:

- The Child Protection and Safeguarding Policy
- Behaviour, Sanctions and Rewards Policy
- Anti-Bullying Policy
- Staff Handbook

The school will, where appropriate, inform parents of incidents of inappropriate online behaviour that take place out of school.

E-Safety in the Curriculum

Online safety must be a focus in all areas of the curriculum and staff should reinforce these messages across the curriculum. The e-safety curriculum at the school is broad, relevant, provides progression, and will be provided in the following ways:

- An e-safety curriculum is provided as part of ICT, PSHE and other lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and external speakers.
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school.
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging.
- Pupils are made aware of the impact of cyber-bullying. See also the Child Protection and Safeguarding Policy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

Parents play an essential role in the education of their children and in the monitoring / regulating children's on-line behaviours. The school provides information and awareness to parents through seminars, newsletters and other methods as appropriate.

It is essential that all staff who are granted access to the school network receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by the Deputy Head Pastoral and Head of IT and STEM. All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety and Acceptable Use of ICT Policy.

Further information on the teaching of e-safety and pupils' use of ICT may be found in the school's E-Safety policy.

2. Roles and Responsibilities

Senior Leadership Team

The Senior Leadership Team have a duty of care to ensure the safety (including online safety) of members of the school community. The Headmistress and Deputy Head Pastoral (DSL) are responsible for:

- The review of logs on CPOMS
- Regular monitoring of the filtering systems alongside the IT Manager/Network Engineer.
- Discussion of e-safety at relevant Governors' meetings.

Head of IT and STEM

The Head of IT and STEM is responsible for ensuring that:

- The staff have had adequate training to be able to access and use the wide range of digital structures utilised at the school.
- All hybrid and remote learning is functional and accessible to both staff, students and parents.

IT Technician and Managed Service Provider (Infaserv)

The IT Manager/Network Engineer is responsible for ensuring the following:

- That the school's technical infrastructure is secure and not open to malicious attack.
- That the School meets all e-safety technical requirements.
- That users may only access the school's networks and devices if properly authorised.
- That the filtering policy is applied and updated on a regular basis.
- That monitoring software and systems are kept up to date.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety issues.
- They have read, understood, and agreed to this Staff AUP agreement.
- They report any suspected misuse or problem to the appropriate person for investigation.
- All digital communications with other staff, pupils and parents are on a professional level.
- They help pupils understand and follow the e-safety and acceptable use policies.
- They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Any breach of this policy will be taken seriously and may result in disciplinary action. A member of staff who deliberately or recklessly discloses personal data held by the school without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

3. School Systems and Technical Information

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. The IT Technician and Managed Service Provider continually reviews and audits the safety and security of school technical systems. Servers, wireless systems and cabling must be securely located and physical access restricted. Data is backed up regularly and securely encrypted. Internet access is filtered for all users via Watchguard and ContentKeeper. The firewalls regularly check for an updated filter list.

All web access is logged. Staff web access to restricted categories is also logged, including when school devices are offsite. Users are made aware of this in this agreement and relevant staff induction. Security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts that might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date anti-virus and anti-malware software.

4. Security

Information security is the most important aspect of data protection compliance. Most of the fines under the Act relate to security breaches such as leaving an unencrypted memory stick in a public place, sending sensitive documents to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web.

Under the Act, personal data is defined as:

- Personal information that has been, or will be, word processed or stored electronically (e.g. in computer databases and CCTV recordings). If a record containing Personal Data is held on a computer, then it will be covered by the Act. This is the case regardless of how the information is held. For example, personal data stored in an e-mail, in a spreadsheet or on a smartphone, are all covered by the Act.
- Personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, department, pay details). Some paper records are not covered by the Act although there are so many exceptions that best practice is to treat all paper records as being covered.
- Some health records prepared by a doctor, nurse, or other health professional (even if not held on computer or held as part of an organised file).

The Act requires the school to take organisational measures (for example, ensuring that staff are trained on information security), and technical measures (for example, encryption, secure shredding etc) to ensure that personal data is kept secure. Staff must ensure that their use of personal data is necessary and proportionate. For example, staff must not take personal data off School premises unless there is a genuine need (subject to the other provisions of this policy). Any devices taken offsite are required to have security locks or codes to prevent access in case of loss or theft. In the event of theft or loss, the IT Technician and Managed Service Provider must be informed immediately to ensure the devices are locked or disabled.

Staff are required to take all necessary steps to prevent unauthorised access to information held on the school's ICT systems. Extra care should be taken with data that is classified as Sensitive Personal Data under the Act. Sensitive personal data is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity.

Staff must be very careful when sending correspondence containing personal data (e.g. sending a fax, an e-mail, or sending documents by post). Staff should check at least three times that they have got the address correct. If the communication contains sensitive personal data or is particularly confidential then staff should take extra precautions such as asking a colleague to check that the number/e-mail address has been entered correctly. Staff should not share the personal details of others without prior consent. This is particularly important when sending e-mails to multiple recipients. The BCC function should be used to protect e-mail addresses. Staff must not use or leave computers, portable electronic devices, or papers where there is a significant risk that they may be viewed or taken by unauthorised persons.

Staff should take reasonable steps to ensure that such devices are not viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased. Staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password secure. In the unlikely event of password security being breached, users must immediately change their password and inform the IT Technician and Managed Service Provider. Staff must not share their passwords with anyone else. Staff will be required to reset their passwords on a regular basis.

No devices should be left unattended or unsecured when a member of staff is logged in. To prevent unauthorised access, users must either logout or lock the screen when leaving a classroom.

Remote access via Microsoft 365 (**MS365**) is the preferred route for accessing school information remotely. Staff must ensure that their use of the school's systems remotely does not compromise the security of the network, and that files containing personal data of staff/pupils are not downloaded or retained onto their personal devices.

Staff must immediately report all security incidents, breaches, and weaknesses, to the Headmistress and the IT Technician and Managed Service Provider. This includes anything which the member of staff becomes aware of even if they are not directly involved (for example, if a teacher notices that document storage rooms are sometimes left unlocked at weekends). Any loss or theft of the school's data must also be disclosed immediately.

Printed material of a confidential nature, which links any pupil to the school, should be printed in a secure area. Printed material of a confidential nature which links any pupil to the school should not be kept for longer than is necessary and be disposed of using a shredder bin in the office.

Staff should exercise caution when opening e-mail attachments, as these may contain viruses. E-mails from unknown sources, or from known sources which seem "out of character", should be treated with extreme caution. If in doubt, advice should be sought from the IT Technician and Managed Service Provider.

With regards to the security of personal data held on any device, staff must ensure that encryption is used in all cases. When sending confidential information by e-mail to an external recipient, it must be encrypted with a password which should be communicated separately by telephone.

With regards to the security of Personal Data held in physical form, staff must:

- Ensure that any such records are kept under lock and key in a secure location.
- Take extra precautions in relation to any Sensitive Personal Data (as defined above), and any Personal Data which is particularly confidential, both of which should be stored in a storage room or in a strong cabinet (again under lock and key).
- Ensure that documents containing Personal Data are never left unattended on desks (unless the room is secure).

Passwords

All users are provided with a username and required to set a secure password. Users are responsible for the security of their username and password. Passwords must follow the guidelines and policies set by the IT Technician and Managed Service Provider and staff are responsible for keeping their passwords secure by means of the following:

- Ensuring not to write it down on a piece of paper or book that is easily accessible or visible (e.g. at your desk or stuck on a note to your monitor).
- Not storing login credentials on a personal computer, mobile device or phone on software that is easily accessible.
- Never share your work password or login credentials with anyone.
- Ensuring that any school information accessed from their PCs or removable/ portable media equipment is kept secure.
- Lock all screens before moving away from their computers to prevent unauthorised access. (Using Ctrl + Alt + Del -> Lock or by using Windows Key + L)
- Screens should be kept out of view of pupils or third parties when accessing personal, sensitive, confidential, or classified information
- All password for school systems must contain a minimum of 8 characters including a mix of lower case, upper case and numbers

Two Factor Authentication (2FA)

Staff will be expected to use two factor authentication for critical pieces of software, such as iSAMS, CPOMS & MS365. They will need to set up a personal device, such as a smartphone, with a 2FA app, such as Microsoft Authenticator and/or Google Authenticator. These are then used to provide a second layer of security for logging into services.

Social Engineering and Phishing Scams

Social engineering and phishing scams are a major source of compromised account credentials. These are eternal attacks that trick the user to reveal their account information. These attacks can be via phone, text, or e-mail. A common form of attack is a disguised e-mail that looks legitimate requesting a user to reset or provide account login credentials. The e-mail could contain a link or fraudulent login page directing the user to provide login credentials. In some cases, the link may contain embedded malicious code that gets installed on the user's computer.

Users must not provide any account authentication credentials (both account login name and password) via e-mail or text. Users must not reset account credentials via website links other than those systems that are solely used by the school.

Brute force attacks

Dictionary and “brute-force” attacks are techniques used by attackers to guess insecure passwords to gain access to a system. Passwords that are generated or created poorly are the most susceptible to being compromised. Users must not use easily guessed passwords such as pet’s names or common words, etc.

Public kiosks or untrusted devices

Credentials are at high risk when used on public kiosks (hotels, airports, etc.) and on untrusted devices (friends or family devices). You may forget to logout and the next user may obtain your credentials; or the device may have already been compromised with malware that can obtain your credentials. Do not login to School systems from public kiosks or untrusted devices.

iSAMS

The school is a data controller and therefore all data stored in iSAMS must be handled in accordance with GDPR guidance. Staff are individually responsible for following this guidance in their use of iSAMS.

Use of Digital Images/Video

The taking, storage and use of images is an important aspect of the use of ICT. All pupils and staff should be aware of the potential sensitivities in this area, and the implications for both safeguarding and data privacy. Please see Images of Children Policy or more details. In accordance with guidance from the Information Commissioner’s Office, parents are welcome to take videos and digital images of their children at school events for their own personal use, but these images should not be published on social media or other channels.

School Website

The Headmistress takes overall responsibility to ensure that the website content is accurate, and the quality of presentation is maintained. Uploading of information is restricted to our website administrators and office staff. The school website complies with the statutory DfE guidelines for publications. Most material is the school’s own work; where other’s work is published or linked to, credit is given to the sources used and clearly state the author's identity.

Photographs published on the web do not have full names attached. We do not use pupils’ names when saving images in the file names or in the tags when publishing to the school website. We do not use embedded geo-data in respect of stored images. Teachers using school approved blogs or Wikis are expected to password protect them.

5. E-mail and Communication

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including direct written contact between schools on different projects, be it staff-based or pupil-based, within school or international.

The school provides staff with an e-mail account for their professional use and makes clear that personal e-mail should be sent through a separate account. The police may be contacted if staff or pupils receive an e-mail that is particularly disturbing or lawbreaking. The school e-mail service may be regarded as safe and secure. Users should be aware that e-mail leaving or entering the school is scanned for viruses, spam, and bad language.

- Staff only use the school's e-mail systems for professional purposes.
- Use of external personal e-mail accounts should be limited during School hours.
- Staff will be made aware that e-mails sent to parents, or an external organisation must be written carefully.
- The sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used.
- Where there is a direct link to a school e-mail account set up on a personal device, such as a mobile phone, this must be secured with a complex password.
- Staff should note that the school may be required to disclose internal e-mail communications to third parties, for example, if a parent makes a subject access request under the Act.

Children in Year 3 to 6 can use e-mail internally to send their teachers an email and to use MS365 applications, including Teams (see below) and are guided in the use in computing lessons. Incidents of inappropriate language are flagged by the school's digital monitoring software provided by Content Keeper.

MS365 and Teams

Teams are the digital equivalent of classrooms and must be treated as such. These must never be set to public and must always be set to private. The teacher who is in the owner of the Team is responsible for the management of the Team and the content posted on that Team. The teacher, in liaison with the Deputy Head Pastoral and Head of IT and STEM, also has a responsibility to understand how to secure and maintain a functional Team, limiting inappropriate dialogue and ensuring that the digital learning environment is reflective of the standards we hold for our physical learning environments.

6. Social Media

Staff members must be conscious at all times of the need to keep their personal and professional lives separate. School staff will ensure that in private and public use:

- Staff demonstrate responsibility and act with integrity in relation to the school.
- No direct reference should be made in social media to pupils, parents, carers, or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Do not communicate via personal e-mail addresses or accept friend requests from present or past pupils, who are unrelated to you, before they reach the age of 18.
- They do not post comments or photographs which could bring into question their professional credibility.
- Failure to comply with the policy relating to social media may result in disciplinary action.

Online interaction in an 'open' environment such as the School Blogs and Twitter feeds may be appropriate, but still require professional judgment. It must be assumed that whatever is written online anywhere cannot be deleted in the future.

7. Personal Mobile Phones

Staff are required to ensure the following:

- Mobile phones and personally owned mobile devices brought into School are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or mobile devices.
- Mobile phones and personally owned devices will not be used in the presence of children during lessons, duties, or other formal school time. They should be switched off or silent at these times. The exception is for SLT and IT Technician and Managed Service Provider who may use their mobile phones for the purposes of communication and emergency response.
- Mobile phones may be used in an emergency when working at an off-site location, such as Beit Hall, Ethos Pool, Battersea Millenium Arena, Fulham Pools or Kensington Gardens.
- No images or videos should be taken on mobile phones or personally owned mobile devices. School-provided equipment should be used exclusively for this purpose.
- All mobile phone use is to be open to scrutiny and the Headmistress is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The school may in exceptional circumstances require access to your device (and any school related information contained in the device). If requested by the school, you must hand over the device and give the school any information (such as any password) necessary to access the device and remove any School Personal Data.

- The school would only make this request if investigating a serious incident or allegation such as a serious security breach involving the device.
- Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people, or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required.

Where staff members are required to use a mobile phone for School duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a School mobile phone will be provided and used. School mobile phones are kept in the school office and they will need to be signed in and out when staff leave and return to the school-site. In the event of an emergency where a staff member does not have access to a school-owned device, they should use their own device and hide (by inputting 141 first) their own mobile number for confidentiality purposes.

8. Responding to Incidents of Misuse

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to safeguarding and child protection are dealt with in accordance with the school's safeguarding procedures. All incidents and complaints relating to e-safety and unacceptable Internet use will be reported using CPOMS. This will be passed on to the Headmistress, Deputy Head Pastoral, Head of IT and STEM, and IT Technician and Managed Service Provider. These will be stored securely in the school's **Pastoral Team**. Incidents of inappropriate language and internet use will be captured by Watchguard and ContentKeeper (the school's monitoring software) and reviewed by the Headmistress/Deputy Head Pastoral. Matters relating to a member of staff will be referred to the Headmistress for action.

Incidents involving the Headmistress will be referred to the Chair of the Board of Governors. Online safety incidents involving safeguarding issues will be reported to the Designated Safeguarding Lead (usually the Deputy Head Pastoral). If a pupil or teacher accidentally opens a website that has content which is distressing, upsetting or inappropriate to the pupils' age, teachers should immediately close the screen and reassure pupils that they have done nothing wrong. The incident should be reported to the Headmistress or Deputy Head Pastoral, including details of the website address and URL.

If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Headmistress immediately. A note of any action should be recorded on the *E-Safety Incident Report Form* (see Appendix 5). All incidents relating to pupils' online safety should be recorded on CPOMS. Any incidents relating to a member of staff will also be recorded in a log maintained by the Headmistress. The incident log will be monitored termly by the Headmistress, a member of the Senior Leadership Team or the Chair of Governors.

Under the Prevent Duty, the school recognises its responsibility to prevent children from being drawn into terrorism and becoming radicalised. The internet and social media have become major factors in the radicalisation of young people. The school teaches about online safety in computing and PSHE lessons. There is appropriate filtering software in place through Watchguard and ContentKeeper to prevent pupils accessing inappropriate websites and social media. Any incidents or concerns staff have about pupils viewing online material relating to radicalisation should be reported to the DSL in line with the school's safeguarding procedures.

Appendix 1:

Glendower Preparatory School

Acceptable Use Agreement (Prep)

ACCEPTABLE USE AGREEMENT FOR SCHOOL DEVICES – PREP

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 a device 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 (Reception and Pre Prep)

ACCEPTABLE USE AGREEMENT FOR SCHOOL DEVICES – RECEPTION AND PRE PREP

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 IT and STEM 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	
IT Technician and Managed Service Provider (Infaserv)	
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 IT and STEM, 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