GIRLINGTON PRIMARY SCHOOL

Online Safety Policy

Date Policy Written:	Autumn 2023
Date Policy Ratified:	Autumn 2023
Date Policy to be Reviewed:	Autumn 2025

GIRLINGTON PRIMARY SCHOOL	Reviewed By
(Non-statutory) D72 **Online Safety Policy** Appendix A –Online Safety Incident Log Appendix B –Technical Infrastructure and support. Appendix C –Cyber Security Appendix D –Website Request Form Appendix E –Responding to online safety incidents	Online Safety Team _____

This policy applies to all members of Girlington Primary School (staff, students, volunteers, parents/carers and visitors) who have access to and are users of the school ICT facilities (computers, school network, internet) both in and out of the school.

This policy should be used along with:

- Child Protection and Safeguarding
- Acceptable Use Policy – Staff & Volunteers
- Acceptable Use Policy - Students
- Data Protection Policy

Policy Statement

Safeguarding is a serious matter; at Girlington Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safety is an area that is constantly evolving and as such this policy will be reviewed on a regular basis or in response to an online safety incident, whichever is sooner.

The primary purpose of this policy is:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Girlington Primary School website; upon review all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A Student Acceptable Use Policy will be emailed to parents at the beginning of each school year.

The school will monitor the impact of this policy using

- Logs of reported incidents
- Web filtering and reporting
- Use of the Securus monitoring software
- Surveys /questionnaires of students, staff and parents

Roles & Responsibility

Headteacher

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer will oversee online safety in school.
- All Online Safety incidents are dealt with promptly and appropriately.

Governors

A member of the Governing Body has taken on the role of online safety Governor, the role of the online safety Governor will include:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
- Meet with the online safety officer

All Staff

Staff are to ensure that:

- Any online safety incident is recorded in the Online Safety incident log (See appendix A), and reported to the Deputy Head Teacher.
- Any inappropriate sites reported to the ICT Technician.
- Request to be made to the technical staff to permit a website.
- They understand and accept the online safety policy and the Acceptable Use Policy. (Acceptable Use Policy – Staff)

Online Safety in Early Years

The term 'Online Safety' is used to encompass the safe use of all forms of information and communication technologies. The aim, through Online Safety, is to reasonably safeguard all users of such technology from potential known risks.

We approach Online Safety in the Early Years with three guiding principles.

1. *Guided Educational Use*

   Internet use should be carefully planned and targeted within a regulated and managed environment. Children are taught how to ask for help if they come across material or persons who make them feel uncomfortable.

2. *Risk Assessment*

   We have a duty to ensure children in the EYFS are not exposed to inappropriate information, materials or people who may cause harm.

3. *Responsibility*

   Online Safety depends on practitioners, parents, carers and visitors taking responsibility for the use of the Internet and other forms of information communication technologies.

Photographs in Early Years

In Early Years Foundation Stage; practitioners use photographs as a means of capturing evidence of learning as well as stimuli for children to celebrate achievement.
Cameras and iPads are provided to practitioners in order for them to capture this. Under no circumstances should cameras or other photographic technologies be used other than those provided by school unless expressed permission has been sought from the Senior Leadership Team.

Permission to take photographs of children is required from Parents and permission is sought for different means, for example; learning journey, in school displays and school website.

Mobile Phones in Early Years

Please use the school's Mobile Phone Policy in conjunction with this policy.

Restricted and Designated Mobile Phone and Camera Zones in Early Years

Within the Early Years setting there are zones in which cameras, iPads and mobile phones are not permitted. If mobile phones are to be used in an emergency, there is a designated zone in which calls may be answered/made. Restricted zones are identified using icons

All Students

Online safety is embedded into our curriculum and students are given the appropriate advice and guidance by staff, this is done through online safety lessons, school collective worship and cyber awareness workshops.

All students are fully aware how they can report areas of concern whilst at school or outside of school. All students must agree to the policy (Acceptable Use Policy – Students) at the beginning of each academic year.

Online Safety Officer/Deputy Head/ICT Technician

The online safety Officer/deputy Head and ICT Technician will:

- Keep up to date with the latest risks to children whilst using technology.
- Meet with the online safety group on a termly basis.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all online safety matters.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Engage with parents and the school community on online safety matters at school.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Make aware technical support of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Online safety group

Chaired by the online safety officer, the online safety group is responsible:

- to advise on changes to the online safety policy.
- to monitor network/internet/incident logs.
- to establish the effectiveness (or not) of online safety training and awareness in the school.
- to recommend further initiatives for online safety training and awareness at the school.
- to meet on a termly basis.

Name	Position	Speciality	Online safety role
Francesca Watling	Teacher	PSHE Education	Officer
Sarah Arthur	Inclusion Manager	Safeguarding	Member
Zartashia Ishaq	Teacher	Computing	Member
Balal Butt	ICT Technician	Technical support	Member
Tina Butler	Chair of Governors	School Governor	Member

Parents and Carers

Parents play the most important role in the development of their children. Through parents meetings, emails, information on website and school newsletters the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand that the school rules are in place to ensure that their child can be properly safeguarded. As such parents will receive a copy of the Acceptable Use Policy before students access any school ICT equipment or services.

Parents /carers are asked to read through the student acceptable use policy on behalf of their child.

Technical Support Staff

Technical support staff are responsible for:

- The schools technical infrastructure is secure and not open to misuse or malicious attack.
- All windows operating devices are regularly updated
- Filtering levels are applied
    - Blacklist - block websites
    - Whitelist – permit websites
- Anti-virus is fit for purpose, up to date and applied on all devices.
- Passwords are applied correctly to all users (minimum of 8 characters, includes capital letters, numbers characters lowercase letters)
- Ensure any external hard drives, USB's brought into school are scanned for any viruses.
- Ensuring that software licences are kept up to date.
- Internet access is filtered to all users.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- An appropriate jobs system is in place (installed on all staff user desktops) for users to report any technical job requests.
- Monitoring and reporting system is setup and running.

Refer to Appendix B Technical Infrastructure and Support

Technology

Girlington Primary School uses a range of devices, in order to safeguard the students and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering

We use Netsweeper web filtering and reporting software which is provided by Schools Broadband who are part of the Internet Watch Foundation (IWF). The Netsweeper filtering software prevents unauthorized access to illegal websites, it also prevents access to inappropriate websites. The school has control to filter themselves to permit or deny access to specific websites. The filtering system is applied on the network and has the ability to provide information on websites visited by users. The Deputy Head and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Please see appendix D, this is form must be completed by staff who wish to block or unblock websites.

Emails

We are currently using Microsoft Exchange for our emails. All email accounts are managed by the IT Technician using Microsoft 365. All staff are required to use their school email accounts and not personal email accounts. The school has the ability to manage email accounts.

If sending emails or texts from school, staff should ensure they do not include their pupils' full name.

Monitoring Software

We use Securus for our monitoring and reporting. If a child is in breach of their acceptable use agreement whilst on the computer then an email is sent to the designated people with a screen shot of the incident showing what was displayed at that time and who was involved (Appendix C: Responding to online safety incidents).

Encryption

All school laptops are encrypted using Bitlocker. No data is to leave the school on an un-encrypted device.

Passwords

All staff and students are unable to access any devices on the school network without a unique username and password. All staff are asked to create a password minimum of 8 characters (mixture of uppercase letters, lowercase letters, numbers and symbols).

All staff are not to disclose their passwords to anyone, nor write down their passwords.

Supply teachers are given their own username and passwords but are limited on the school network, the passwords are regularly changed.

Anti-virus

Sophos Antivirus software is installed on all Windows operating system devices and is set to run on a regular interval. Although some windows features have been disabled to help prevent viruses, in some cases if a computer is infected with a virus it will be flagged on the Sophos Control Console and appropriate action will be taken

Use of photographs on school website and other media

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.

- There is to be no identification of students using first name and surname; first name only is to be used.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents – if any incident occurs the Deputy Head will assist staff in taking the appropriate action and to fill out an Online Safety incident log. An email is also sent to the designated people automatically with a screen shot of the incident showing what was displayed at that time and who was involved.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Girlington Primary School will have an annual programme of training which is suitable to the audience.

Online safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head teacher for further CPD.

Appendix A **Online Safety Incident Log**

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Deputy Head)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature		**Date:**	

Appendix B

Technical Infrastructure and support.

The school has a Fortigate network firewall system, web filtering system and a monitoring system in place. The Netsweeper system allows the technical support to manage the web filtering, permit/deny websites. Securus (monitoring security systems) allows the technical support to monitor user activity.

The servers, network cabinets, wireless control, modems and routers are all kept secure with restrictions on access.

The school employs a full time technician, to take responsibility with the general maintenance of the school network, which includes: laptops, computers, printers, web filtering, software installation and servers. The school has a contract with Sims.Net support, and an additional contract with an IT support engineer to come onsite and assist the technician.

The Technical support staff has the following duties and responsibilities:

- To ensure all Windows based operating system is deployed on all computers.
- Sophos Anti-virus software is installed on all computers and is run and updated on a regular interval.
- To keep up to date with Sims.Net
- To keep all computers up to date with the latest version of windows operating system and windows update.
- All networking technologies (servers, routers, switches and DVR) are securely located and physical access is restricted to IT support only.
- Passwords to the servers are restricted to the school technician, school admin, Primary Technology (IT Support) and Schools ICT (Sims Support).
- All servers are backed up and monitored offsite by Primary Technology.
- Servers are monitored by the onsite technician and Primary Technology this allows the company to monitor/report to the onsite technician.
- Primary Technology assist and advise the school on any security updates, network issues and upgrades.
- All users are defined in groups (Management, RP, Teachers, Admin, and Pupils etc.) and are given access rights accordingly.
- Software is in place in the ICT suite (LanSchool), this allows the staff member to control workstations and view user activities.
- Web filtering and reporting system is in place for safeguarding against any inappropriate websites. The onsite technician has the control to permit/deny any websites.
- School has a monitoring and reporting system in place.
- An appropriate jobs log is in place (installed on all staff user desktops) for users to report any technical job requests.
- An agreed policy (Acceptable use policy – Staff) is in place regarding the extent of personal use of school equipment by family members.
- Users are not permitted to download any software, any request for software installation is logged in the jobs log system and reported to the technician. The software is then deployed on the school network according to the licence agreement.

- Users will be responsible for the security of their username and password and must not allow others to access the systems using their log on details.
- All users are required to lock their workstations when away from their desk.
- Users must immediately report any concerns where they feel that there has been a breach of security.
- All user log on details (access to school network, email accounts, Sims) are removed once the user has left the school.
- To ensure that all visitors are connected on the school Wi-Fi as a guest user, which will give them access to the internet only.
- All lost or misplaced school It equipment e.g laptop, ipad etc must be reported to the IT Technician.

Appendix C

Cyber Security

Over the years schools have become very reliant on technology from emails, websites, school databases and online lessons plans. If a Cyber Incident was to occur this would have a major impact to the school.

What is a Cyber incident

A cyber incident or attack is when:

- Unauthorised user had gained access to your systems/data
- Changes to system are made without consent
- System/data is encrypted by the attacker
- An attack causes the system/network to run slow or crash

What are the types of Cyber incidents

Phishing attack

Phishing is where an email appears genuine but is actually fake. It might try and trick you into revealing sensitive information, or it might contain a link to a malicious website or an attachment that is infected with malware. Some phishing attempts are random, while others might be more targeted to you as an individual, or to specific organisations like schools

Phishing attempts typically arrive via email but can also arrive by: social media, text message or phone call.

Ransomware

Ransomware is a type of malware that spreads into your network and encrypts all data and computers like the WannaCry ransomware attack on the NHS in May 2017.

Once all the data and computers have been affected the attackers then demand a payment in exchange for the decryption key.

Denial of service (DOS)

This is when the attacker sends lot of traffic/information to the network causing the network and server to run slow or crash.

How to keep safe online (NCSC)

5 keys ways to defend against cyber incidents *(recommended by the National Cyber Security Centre (NCSC)*

1. **Defend yourself against phishing attempts**
   If you receive phishing emails, text messages or on your social media accounts look out for the following:
   - Spelling and grammar mistakes
   - Sense of urgency e.g Urgent attention needed
   - A link that doesn't match the destination

- An attachment with no description or strange name
- The full email address that doesn't match the destination

If you receive an email that has any of the above or you are unsure delete it

2. **Use strong passwords**
    - Refer to the schools Online Safety for creating and using passwords
    - Renew your passwords every 3 months
    - Use separate password for your work and home accounts
    - Switch on 2 factor authentications if you have this
    - Store password securely e.g password manager, google chrome

3. **Secure your devices**
    - Do not ignore updates (windows/ios/andriod)
    - Only download updates from trustworthy sources (Apple store, Google Play & windows update)
    - Lock your devices when not in use (iPads, laptops/computers)
    - Encrypt all your devices laptops, USBs

4. **If in doubt call it out**
    - Report any suspicious activity

Disaster recovery plan

In case of a cyber incident or network failure Girlington Primary School has a disaster and emergency recovery plan for IT failure and this can be found in the schools Emergency Plan.

Take all necessary measurements outlined in the emergency plan.

All staff and at least one Governor to take an annual mandatory Cyber Security Training from the 'National Cyber Security Centre' recommended by the Department of Education.

Appendix D

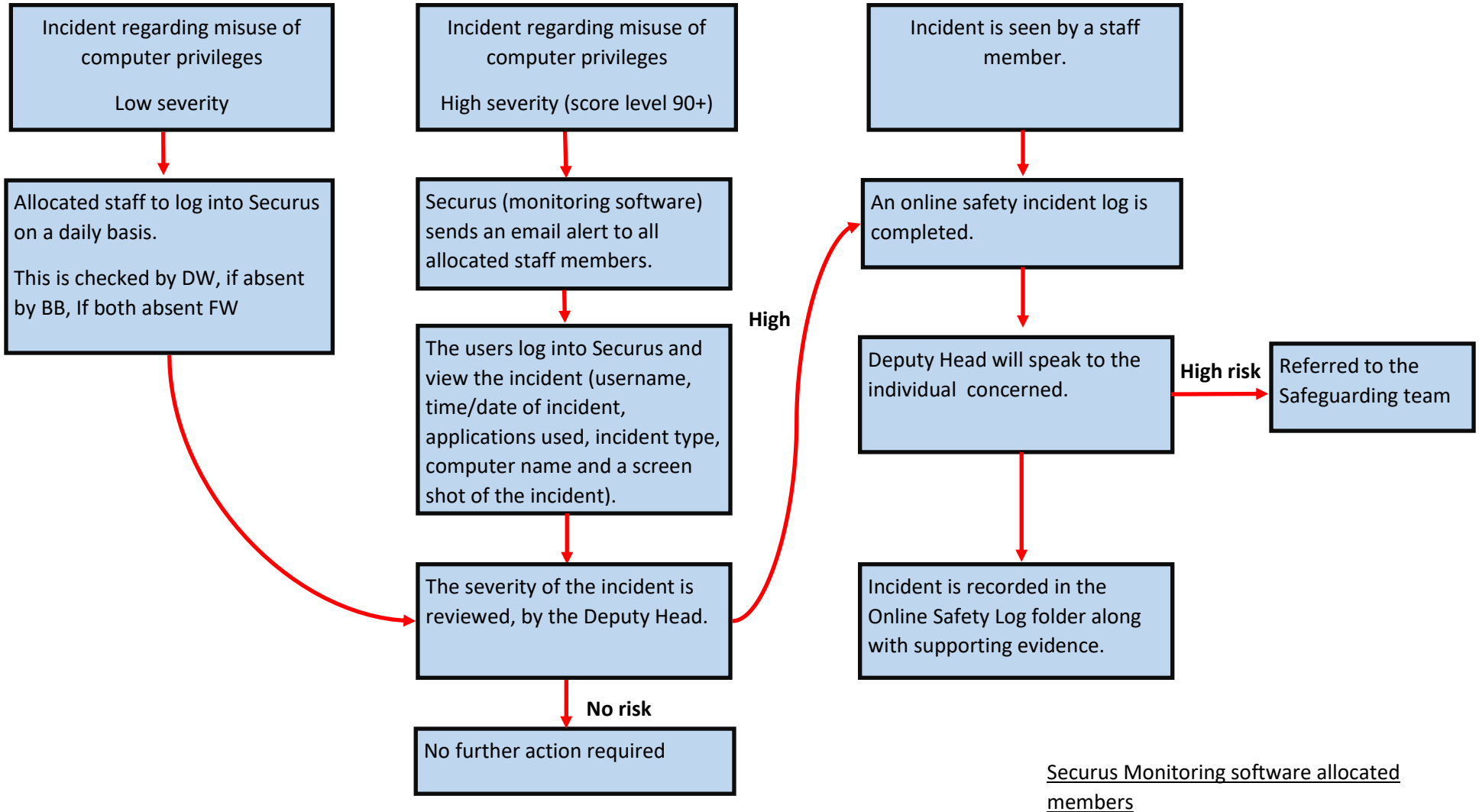
Website Request Form

Number:	**Name:**	**Date:**	
Website Information			
Website Name:			
Website URL:			
Type of Request (please tick relevant box)			
Block website		**Unblock website**	
Reason for the request (teaching subject in class, or inappropriate website)			
When required?			
Duration required for: (few days, permanent)			
Office use only			
Signed:		**Date:**	

-

Appendix E

Responding to online safety incidents



<u>Securus Monitoring software allocated members</u>

Online Safety Officer – *Mrs F. Watling (FW)*

Deputy Head - *Mr D.Walker (DW)*

IT Technician - *Mr B.Butt (BB)*