GODWIN JUNIOR SCHOOL

Online Safety Policy

Date agreed by Governors	Autumn 2014
Reviewed	Autumn 2015
Reviewed	Autumn 2017
Reviewed	Autumn 2018
Reviewed	Spring 2021
Next Review	**Spring 2022**

Linked Documents
Acceptable Internet Use Policy
Child Protection and Safeguarding Policy
Prevent Policy
Staff Handbook
Computing Curriculum
Computing Policy
Data Protection Policy
CCTV Policy

RIGHTS
RESPECTING
SCHOOLS

unicef
UNITED KINGDOM

SILVER – RIGHTS AWARE

The United Nations Convention on the Rights of the Child (UNCRC) articles which inform this policy are:

- Article 3: The best interest of the child must be top priority in all decisions and actions that affect children
- Article 12: Every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.
- Article 16: Every child has the right to privacy.
- Article 17: Every child has the right to reliable information and to be protected from material that could harm them.
- Article 19: Children must be protected from all forms of abuse by those who look after them.
- Article 28: Every child has the right to education. Discipline in schools must respect children's dignity and their rights.
- Article 29: Education must develop every child's personality, talents and abilities to the full. It must encourage the child's respect for human rights, as well as respect for their parents, their own and other cultures, and their environment.
- Article 31: Every child has the right to relax, play and take part in a wide range of cultural and artistic activities.

School's Purpose: To prepare pupils for lifelong success

School's Vision: At Godwin Junior School we:

- Value everyone
- Instil a love of learning
- Seek and encourage talent
- Inspire resilient learners
- Open minds to develop responsible global citizens
- Nurture confident, articulate individuals

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Godwin Junior School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be 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 students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content and misinformation or fake news
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming [sexual exploitation, radicalisation, catfishing (creating a fake identity to target an individual for abuse or fraud) etc.]
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright and plagiarism (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of our school IT systems, both in and out of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and available in the school entrance.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable Use agreements discussed with staff and pupils at the start of each year.
- Acceptable Use agreements to be issued to whole school community, on entry to the school.
- Discrete teaching of online safety practices during Computing lessons and assemblies.

Reviewing and Monitoring Online Safety

- The Online Safety Policy is referenced within other school policies (e.g. Safeguarding and Child Protection Policy, Anti-Bullying Policy, Prevent Policy, Computing Policy, Acceptable Use Policy).
- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy; it has been agreed by the Senior Leadership Team and approved by Governors. All amendments to the school Online Safety Policy will be disseminated to all members of staff and pupils.

2. ROLES AND RESPONSIBILITIES

Role	Key Responsibilities
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review its the effectiveness • To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities • The role of the Safeguarding Governor will include regular review with the Online Safety Leader.
Head Teacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety

Role	Key Responsibilities
	roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including the risk of children being radicalised • To receive regular monitoring reports from the Online Safety Leader • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. School-Based Technician • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure school website includes relevant information
Online Safety Leader/Designated Safeguarding Lead	• Take day-to-day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • To communicate regularly with SLT and the designated Safeguarding Governor to discuss current issues • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys/pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and is aware of the potential for serious child protection concerns.
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
School-Based Technician	• To report online safety related issues that come to their attention, to the Designated Safeguarding Lead • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices

Role	Key Responsibilities
	- the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Leader or Head Teacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures
Teachers and Support Staff	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors	• To read, understand, sign and adhere to the school staff Acceptable Use Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the Online Safety Leader • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology Exit strategy: • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gather

Role	Key Responsibilities
	information about their online experiences
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • To actively engage in keeping their child/ren safe when online work is being undertaken at home. • To consult with the school if they have any concerns about their children's use of technology • To support the school in promoting online safety. • To endorse the Parents/Carers' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.
External groups including parent/carer groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • To support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

3. EDUCATION AND CURRICULUM

Pupils

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.
This school:

- Has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to pupils' age and experience.
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind children about their responsibilities through the pupil Acceptable Use Agreement as well as during lessons
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights
- Ensures pupils only use school-approved systems and publish within appropriately secure/ age-appropriate environments

Parents and Carers

Many parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring of their child's online behaviour. Parents/carers may underestimate how often children and young people come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parent/Carer workshops
- High profile events e.g. Online Safety Day
- Asking them to read and sign an Acceptable Use Policy

Staff

It is essential that **all** staff receive regular online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of online safety training will be made available to staff. This will be regularly updated and reinforced. All staff read and sign the Acceptable Use Policy
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Internet Use Agreement and sign to say that they have read the latter.
- Trainee teachers and students on work experience placements will read the Online Safety Policy and sign the Acceptable Internet Use Agreement
- The Online Safety Leader will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- This Online Safety Policy and its updates will be shared with staff

Governors

Governors are asked to develop their online safety awareness sessions through attendance at training provided by NPW or other relevant organisation. They are also invited to participate in school training sessions.

4. EXPECTED CONDUCT

In our school:

All users:

- read and sign the relevant Acceptable Use agreement
- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so
- understand the importance of adopting good online safety practice when using digital technologies in and out of school
- know and understand school policies on the use of mobile and hand-held devices including cameras and other recording apparatus

Staff

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies
- know to take professional, reasonable precautions when working with pupils: previewing websites before use; using age-appropriate search engines where more open Internet searching is required

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety Acceptable Use agreement form
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse

5. EQUIPMENT AND DIGITAL CONTENT

Mobile Devices (Mobile 'phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupil or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any 'phone or handheld device brought into school.
- Pupils who bring their mobile 'phone into school must hand it in to the school office upon arrival in the morning and collect it at the end of the school day.
- Staff members and supply teachers must store their 'phones and other handheld devices in a locker when they arrive at school. These cannot be taken into classrooms or other areas of the school which children have access to. The only exception to this is on school visits where staff would need to be contactable and to have immediate contact with each other and the school if an incident occurred.
- If a member of staff wishes to use their 'phone during the school day this must only be in areas which the children do not have access to e.g. the staffroom. Failure to adhere to this will be treated as a disciplinary matter.
- If a staff member is expecting an urgent personal call they may seek specific permission from the SLT to switch their 'phone to silent and keep it on their person so that they can return the call straightway from an area which the children do not have access to e.g. the staffroom. Failure to adhere to this will be treated as a disciplinary matter.
- All visitors are requested to either store their 'phones in the office of the member of SLT whom they are visiting or switch their 'phones to silent during their time in the school if they must have it on their person (e.g. Social Worker etc) .
- The recording/ taking of images, video and audio on any personal mobile device is not authorised, except where it has been explicitly agreed by the Head Teacher. Failure to adhere to this will be treated as a disciplinary matter.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

6. USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out Internet searches for information about potential and existing employees.

The school will inform and educate pupils about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital or video images of children to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

7. INCIDENT MANAGEMENT

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- There is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- The Online Safety Leader acts as first point of contact for any incident. If he/she is not in school, the Head Teacher should be informed of the incident.
- Any suspected online risk or infringement is reported to the Online Safety Leader (or in this person's absence, the Head Teacher) on that day.
- Any concern about staff misuse is always referred directly to the Head Teacher, unless the concern is about the Head Teacher, in which case the issue is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).
- Support is actively sought from other agencies as needed (i.e. the Local Authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues.
- Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will immediately refer any particularly disturbing or suspected illegal material to the police and inform the LA.
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school.

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the Designated Safeguarding Lead. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response.
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another school, college, setting or individual.
- Whether to contact parents/carers of the pupils involved - in most cases parents/carers should be involved.

An immediate referral to police and/or children's social care should be made if at this initial stage:

- The incident involves an adult.
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent.
- The imagery involves sexual acts and any pupil in the imagery is under 13.
- You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the Designated Safeguarding Lead is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and, if appropriate, local network of support.

8. MANAGING IT AND COMMUNICATION SYSTEMS

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored.
- Has the educational filtered secure broadband connectivity through the LGfL.
- Uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- ensures network health through use of Sophos anti-virus software (from LGfL)
- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users - the LGfL USO system.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Has additional local network monitoring/auditing software installed
- Requires the School Based Technician to be up-to-date with LGfL services and policies.
- Has daily back-up of school data (admin and curriculum).
- Ensures that storage of all data within the school will conform to the EU and UK data protection requirements.
- Ensures that storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to the service is through a unique, audited username and password. We also provide a different username and password for access to our school's network.
- All pupils have their own unique username and password which gives them access to the Internet and other services
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use staff logins.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to log off or lock their device when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up-to-date virus protection.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school is used primarily to support their professional responsibilities.

- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, personnel system etc.
- Maintains equipment to ensure Health and Safety is followed.
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems.
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data.
- Uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Ensures that our wireless network has been secured to appropriate standards suitable for educational use.
- Ensures that all IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards.

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; if a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, LGfL USO admin site twice a year.
- We require staff using critical systems to use two factor authentication.

E-mail

This school:

- Provides staff with an email account for their professional use (LGfL Staffmail) and makes clear that personal email should be through a separate account.
- Uses anonymous or group e-mail addresses, for example info@godwin.newham.sch.uk or class e-mail addresses.
- Will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Uses a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and ‘netiquette’ of using email both in school and at home.

Staff:

- Staff only use LGfL e-mail system for professional purposes.
- Access in school to external personal email accounts may be blocked.

- Should immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Ensure that any digital communication between them and parents/carers is professional in tone and content. These communications may only take place on official, monitored school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Never use email to transfer 'Protect-level' data. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Head Teacher, supported by the Governing board, takes overall responsibility for ensuring that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DFE requirements.
- Photographs published on the website that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Most material is the school's own work; where others' work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Photographs published on the web do not have pupils' 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.
- Personal information is never posted on the school website and individual email addresses are not included.

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Staff are instructed not to run social network spaces for pupil-use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not become online friends with any pupil or former pupil under 18 years of age. Any exceptions must be approved by the Head Teacher.
- 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 or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Learn that they must not take, use, share, publish or distribute images of others without their permission.

- Learn about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Students are required to sign and follow our pupil Acceptable Use Agreement.

Parents/Carers

- Parents/Carers are reminded about social networking risks and protocols through our parent/carer Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they should not upload to social media sites photographs, videos or any other information/comments about pupils other than their own child(ren).

9. DATA SECURITY: MANAGEMENT INFORMATION SYSTEM ACCESS AND DATA TRANSFER

Strategic and operational practices

At our school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised to.
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, or lock it if they will be returning shortly..
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are in lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

10. DATA PROTECTION

Please see our Data Protection Policy for further information.

11. USE OF CCTV AND OTHER AUDIO/VISUAL RECORDING EQUIPMENT

Please see our CCTV Policy for further information.

Online Safety Policy

COVID-19 Appendix

Godwin Junior School is committed to providing a safe environment for online learning. This commitment remains the same in the difficult circumstances brought about by the COVID-19 outbreak. During the period of remote learning our expectations of staff and pupils also remain the same, and the principles and practices of the school's *Child Protection and Safeguarding Policy*, *Online Safety Policy* and staff Code of Conduct will continue to apply, both to existing and any new online and remote learning arrangements introduced. Staff and parent/carers must read these policies and ensure that they adhere to them at all times.
In order to ensure the safety and welfare of children during the period that they are engaging in remote learning, the school will follow the DfE remote learning guidance:
https://www.gov.uk/guidance/safeguarding-and-remote-education-during-coronavirus-covid-19

Given the changes in circumstances to everyday teaching and learning practices, the following guidelines will also apply:

Providing a safe system

- Where the site remains open, the school will continue to ensure that appropriate filters and monitoring systems are in place to protect children when they are online on the school's IT systems or recommended resources.
- For the purposes of remote learning, the primary platforms used are:
    - Google Classroom
    - Zoom
- The platforms are restricted to Godwin families only and permissioned accordingly. Other platforms may be used at times for specific purposes. The online safety implications of any platform are carefully considered before use.
- The school has technical support dedicated to maintaining a safe and operational online environment.
- All staff have day-to-day responsibility for online safety, and will maintain an active oversight of the management of remote learning from a safeguarding perspective. Procedures will be kept under review and action will be taken swiftly if concerns about the use of technologies arise.
- The school will keep in regular contact with parents/carers, updating them as appropriate with information on how the school is providing remote learning, how they can keep their children safe online and any new developments.

Remote learning

There is a wide range of formats for remote learning, including:

- Posting activities for pupils at regular intervals, with pupils posting responses
- Providing recorded materials
- Providing documents
- Directing pupils to web-based resources and activities they can engage with on or offline
- Interactive, live intervention sessions
- Interactive, live pastoral sessions and online registers

Live online support

- Daily live contact during online registration ensures children are ready to access their learning on time, increases engagement and motivation and sets out the expectations for the day
- Live contact is an important part of pastoral support and provides pupils with a direct interface with a familiar trusted figure at a time of significant change and uncertainty. The interactive, live pastoral sessions also give pupils the opportunity to interact with peers and maintain important social connections during a period when they could otherwise become isolated.
- Live online intervention sessions are an important part of this overall package for pupils of all ages. Interaction is an important part of the learning process, and whilst online contact cannot replicate face to face contact, live intervention sessions are particularly helpful for pupils who struggle with retention and have difficulty grasping new concepts. It also allows effective communication, with pupils able to respond to staff questions – and vice versa.

Protocols for staff in relation to remote learning

In order to safeguard pupils and staff, live online sessions must be conducted following the protocols set out below:

- Familiarise yourself with relevant policies around safeguarding, acceptable use, data protection and conduct.
- Share a class timetable for remote learning
- Protect your personal data
- Only use school-approved platforms; do not use social media in communicating with pupils
- Reinforce online safety messages regularly in your sessions
- Bear in mind the current circumstances and how they are affecting children and families when setting expectations of pupils
- Consider online safety when sharing resources – vet websites and videos/apps/software carefully and bear in mind that the home environment will not have the same content filtering systems as at school. If introducing new apps and resources, ensure these meet GDPR requirements. Contact the Head Teacher for further guidance.
- If concerned about online safety/resources, check with the Head Teacher
- Ensure that passwords and secure information are kept confidential

- Adhere to copyright and GDPR guidelines
- Continue to look out for signs that a child may be at risk – which may differ from typical triggers in a school environment. Report any concerns in the usual way to the DSL without delay
- Do not provide pupils or parents/carers with personal contact details – email, home or mobile numbers, details of web-based identities etc.
- If making calls to families, ensure that calls are made to parents'/carers' 'phones, and that calls are made during school hours as much as possible.
- Do not arrange to meet pupils or ask them to deliver work to your home
- Remain professional and objective in all interactions, including written and verbal
- If providing pre-recorded videos of yourself ensure that you…
    - Record against a neutral background
    - Avoid recording in a bedroom (if that's not possible, use a neutral background)
    - Dress professionally, appropriate for school
    - If sharing your screen, double check that all tabs, windows and other content on the screen is always appropriate for pupils to see
    - Use professional language at all times
- If you encounter inappropriate conduct by children posting publicly or privately on the Google Classroom, Zoom or other curriculum platforms, delete and/or mute offending children (such comments are hidden from view of the class, but are accessible later within Classroom settings), issue a warning privately, and inform the SLT of the incident so that they can discuss with you further action which may need to be taken.
- Do not download and store pupil-identifiable content to a personal computer or device. Keep all pupil content in the protected shared Google Drive environment as much as possible.

In relation to live online sessions:

- Keep a log of live online sessions– date and time, attendance, what was covered, any incidents. Any serious incidents should be reported in the usual manner depending on the nature of the issue.
- Maintain professional conduct during live streaming – dress appropriately, consider your surroundings (background, other household members who may come into view etc.) and blur if necessary and remember that your microphone may be on
- Maintain the same boundaries and insist on the same standard of behaviour as in a school setting. Make specific protocols clear at the outset, e.g. muting of microphones at appropriate times, use of the chat function, etc.

Reporting an issue for staff:

- Any child protection or safeguarding concern must be reported to the DSL without delay
- Concerns about the safety of procedures, behaviours or use of inappropriate technology should be referred to the DSL

- Routine queries about the use of apps or online materials should be addressed to the Head Teacher
- UKSIC's Professionals Online Safety Helpline is a good source of further external advice

Protocols for pupils in relation to remote learning:

- Always log on through your Godwin account and use your Godwin email for remote learning
- Don't share passwords or other personal information
- Do not make recordings, take screenshots/screengrabs or photographs, or store footage of staff or other pupils
- Just like in school, follow the remote learning timetable to keep a routine
- When you communicate using Google Classroom, don't use shorthand; write as though you would speak in class
- Take regular screen breaks
- Only send messages and any pictures or images required for class through Google classroom
- Dress appropriately for online lessons
- Ensure that you have a safe and appropriate place to participate from, preferably not in a room on your own. If you are in a room on your own, leave the door wide open.
- Inform parents/carers about when 'live' learning will be taking place
- Follow the school rules for conduct during online lessons as if you were in school
- Do not undermine in any way the technology used to offer video lessons
- If you have concerns about online safety, or if you feel you are being bullied, talk to someone you trust

Reporting an issue for pupils:

- Speak to a trusted adult
- Ask your parent/carer to email or call the school at info@godwin.newham.sch.uk or 020 85347601
- Contact Childline 0800 1111

The role of parents/carers

- It is the responsibility of parents/carers to ensure that pupils are monitored in their use of technology for remote learning, as they would ordinarily do when their children are using technology at home. Monitoring screen time and having regular breaks are particularly important in the current circumstances
- While pupils are working from home they are connected to their home broadband so their traffic doesn't go through the schools on-line safety filter – parents/carers will therefore need to ensure that age-appropriate filtering or safe search is enabled at home. Information on setting this up can be found at: https://www.saferinternet.org.uk/advice-centre/parents-andcarers/parental-controls-offered-your-home-internet-provider and here: https://www.internetmatters.org/parental-controls/

- Take an active interest in your child's learning and support them as much as possible
- Establish a daily schedule and routine – please refer to the remote class timetable
- Encourage screen breaks
- Ensure your child only communications with staff through our approved school channels – Google classroom and Zoom.
- When pupil learning is taking place help facilitate this to take place in an 'open' space (whenever this is possible). If child is working in a room on their own, please make sure the door is open. Avoid bedrooms if possible.
- Communication during remote learning is between pupil and teacher: parents/carers should communicate with school/staff in the usual manner, via school email or telephone during a period of remote learning
- Social media, networking apps and gaming platforms are particularly popular. Parents/carers are advised to be mindful of age restrictions and to oversee their child's social media activity
- Familiarise yourself with relevant school policies
- The school will update parents regularly regarding online safety matters. Parents/carers are requested to follow the school's advice and contact the school if they have concerns or encounter risk online

Reporting an issue for parents:

- Contact the school on info@godwin.newham.sch.uk or call us on 0208 5347601

Sources of support and advice

UK Safer Internet Centre https://www.saferinternet.org.uk/ - includes a range of activities for children of different ages
CEOP / Thinkuknow https://www.thinkuknow.co.uk/ - includes a range of home activity packs
National Online Safety https://nationalonlinesafety.com/ - Good guides for parents and staff
Parent Info https://parentinfo.org/ - specifically aimed at parents
Internet Matters https://www.internetmatters.org/ - specifically aimed at parents
Net Aware https://www.net-aware.org.uk/ - NSPCC's advice on online matters