# The Clara Grant Primary School
# Online Safety Policy

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

September 2021

# Contents

# 1. Introduction to e safety

Our e safety Policy has been written by the school, building on The London Grid for Learning (LGfL) Exemplar Policy and other example policies and documents.
It has been discussed with staff, agreed by the senior management and approved by the Local School Committee(LSC).

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.
This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

# 2. Policy evaluation and revision

This policy will be revised annually.
(The teaching and learning of e safety by pupils is a statutory part of the Computing curriculum and will be monitored as part of the usual subject monitoring process.)

**Policy completed and agreed:** July 2013
**Last reviewed:** May 2021 and September 2021
**Next review date:** September 2022

There has been a major policy change recently to Data Protection, called GDPR (General Data Protection Regulation). A guide with links has been saved in the E Safety folder alongside this document).
**GDPR in the context of children's data protection at a glance:**
· Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
· If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
· Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
· You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
· If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.
· For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
· Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
· You do not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
· The school should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.

· Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
· An individual’s right to erasure is particularly relevant if they gave their consent to processing when they were a child.
There is a new section in Roles and Responsibility and Technical and hardware guidance in order to migitage a Ransomware attack.

## 3. Context and background

**The technologies**
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information.
Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- email
- Instant messaging
- Web based voice and video calling (e.g. Skype, Meet, Zoom and Teams)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs and Microblogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with email, messaging and internet access

*For more information on the school policy for the teaching and learning of Computing and ICT, please see the Computing and ICT Curriculum Policy.*

## 4. Our whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive safety education programme for pupils, staff and parents

## 5. Roles and Responsibilities

E safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of LSC, aims to embed safe practices into the culture of the school.

**Leadership team**
The SLT ensures that the Policy is implemented and compliance with the Policy monitored. Schools should include e safety in the curriculum and ensure that every pupil has been educated about safe and responsible use.

**e safety Coordinator**
Our school e safety Coordinator is Simone Schwartzel
She ensures they keep up to date with safety issues and guidance. The school's e safety coordinator ensures the Head, senior management and LSC are updated as necessary.

**Local School Committee**
Members of the LSC need to have an overview of e safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e safety and are updated at least annually on policy developments.

**School Staff**
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.
All staff should be familiar with the schools' Policy including:

- Safe use of email;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data - specifically when accessing the network on a personal device. The device will need to have a full version of anti-mallware and virus protection which they can download from the school server. If they want to use a personal device to access the school drive they will need it to be cleared with our School Office manager. An automatic alert has been set on the Drive Admin Console : Any new devices wanting to access the Gsuite will require admin approval. An email will be sent to abibi@claragrant.towerhamlets.sch.uk .
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- publication of pupil information/photographs and use of website;
- eBullying / Cyber Bullying procedures;
- their role in providing e safety education for pupils;

Staff are reminded / updated about e safety matters at least once a year.

**Pupils**
Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with e safety issues, both at home and school. They are asked to agree to a set of guidelines and rules covering their responsibilities when using ICT at school

**Parents**
Parents are given information about the school's e safety policy. They are given copies of the pupil agreement for information, and asked to support these rules with their children.

## 6. Technical and hardware guidance

### School Internet provision

The school uses LGfL (a not for profit service provider to schools in London) as it's Internet Service Provider. LGfL have subcontracted this service to
Virgin Media Business. Virgin provides an always-on broadband connection at speeds up to 100 MB.

### Content filter

The LGfL uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- *All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.*
- *Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.*

### Downloading files and applications

The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Any file or program installation will only be done by a member of the Connetix team.

- Pupils are not allowed to download any material from the Internet.
- Staff and pupils are not allowed to download files from the Internet (unless from a trusted subscription for example Twinkl or Hamilton Trust) , via email programs or USB onto school computers. In the event that a member of staff does download an infected file the following steps need to be taken:
    a. Take the device offline. You can do this by shutting off the Wi-Fi, shutting off your computer, or pulling out the ethernet cord from your computer.
    b. Immediately inform a member of the SLT and or Computing team
- Portable storage media - Portable media USB memory sticks are a common way of introducing a virus or other undesirable agent into a school computer system. They may not be used unless advised by the SLT, Computing Coordinator/technician or by a member of the Connetix team.

### Security and virus protection

The school subscribes to the Sophos Endpoint software program and Malwarebytes both on the workstations and server. Both are cloud based antivirus and anti Malware services that are updated automatically at regular intervals.

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the Computing Coordinator/Computing technician.
- In terms of a ransomware attack, the level of reach is determined by the level of access.
  The great likelihood of being hit is via a staff or student user's account - as their level of access is restricted by network permissions the extent of the damage will be localised to their documents and perhaps a shared folder or two. In these instances, the file-based backup above will resolve the issue the most swiftly.

## 7. e safety for Pupils

We believe it is our responsibility to prepare pupils for their lives in the modern world, and Computing is an integral part of that world. At our school we are committed to teaching pupils to use ICT safely, effectively and appropriately in all aspects of their education.

***Internet access at school***

**Access for all - Inclusion**
All pupils have access to ICT as part of the curriculum. Details of how we manage access to the curriculum for all pupils is contained in our Inclusion Policy

**Use of the Internet by pupils**
Internet access is carefully controlled by teachers according to the age and experience of the pupils, and the learning objectives being addressed.

**Pupils are always actively supervised by an adult** when using the Internet, and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

**Out of Hours Provision**
There will be no unsupervised access to the Internet at any time during Out of Hours provision. Clubs such as Code Club will be adequately supervised while children are accessing the internet.
Google Classroom settings will be set to close the “stream” off at night and on the weekends, teachers will set reasonable “working hours"

## 8. Teaching safe use of the Internet and ICT – Digital Literacy

The safe and responsible use of ICT is now a statutory part of the Computing curriculum introduced in September 2014, and will be taught discretely with age appropriate lessons, activities and resources.

**We teach the following aspects of e safety as part of the Computing Curriculum**
*Please see the Computing and ICT scheme of work for more details.*

| | ***Digital Literacy - Understanding and Using Technology Safely*** |
|---|---|
| **KeyStage1** | ● Know how computers and other devices can be connected into networks with cables and WiFi<br>● Understand and describe some of the ways we communicate with others online<br>● Be able to identify appropriate places to meet and chat online and why they should not to talk to strangers<br>● Know what info they should NOT share with others online<br>● Understand that there are rules about how we should use technology to keep us safe<br>● Be able to discuss how they would ask for help if they felt they needed it |

| | |
|---|---|
| LowerKeyStage2 | ● Know the basic structure of the Internet and World Wide Web and how information travels around it<br>● Use digital communication tools (email, forums etc) safely and appropriately<br>● Use a safe online social space (learning platform) to explore collaboration and networking<br>● Know that there are copyright rules and that information should not be copied without permission<br>● Know about the KIDSMART rules and other e safety portals<br>● Understand that online communication should be responsible and appropriate<br>● Describe how they would ask for help |
| UpperKeyStage2 | ● Understand how information is named, organised, moved and stored on the Internet<br>● Know about some of the key people and events in the history of computing and the Internet<br>● Know about different online communication tools and some of the rules about use by young people<br>● Be able to discuss issues around cyberbullying and appropriate online behaviour<br>● Understand some of the issues around personal data and how it might be used by others if shared online<br>● Know that there are consequences to misusing digital information - eg plagiarism<br>● Be able to explain how they would report concerns about online material of behaviours to the appropriate people |

***Finding Suitable material***
We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material.
Where possible, and particularly with younger children, we provide pupils with bookmarks or create wakelets for suitable sites and staff always check the suitability of websites before using them in teaching and learning.
We evaluate, purchase and provide access to relevant online digital resources libraries, eg Twinkl, Mathletics etc.

***Unsuitable material***
Despite the best efforts of the LA and school staff, occasionally pupils may come across something on the Internet that they find offensive, inappropriate, unpleasant or distressing.

Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. The action will include:

1. Logging the incident and making a note of the website and any other websites linked to it
2. Informing the Computing Coordinator/Network manager and Head teacher
3. Informing the Trust/LEA/Internet Service Provider so that the website can be added to the content filter
4. Discussion with the pupil about the incident, and how to  avoid similar experiences in future
5. Discussion with parents if felt necessary

***Using Email at school***
Email is a valuable and stimulating method of communication that plays an important role in

many aspects of our lives today. We believe it is important that our pupils understand the role of email, and how to use it appropriately and effectively.

- We teach the responsible and safe use of email as part of our Computing curriculum
- Pupils are taught that email messages sent using a school account will represent the school as well as the pupil, and that they should take care to act respectfully and appropriately
- Any email links set up by the school will be carefully checked, monitored and controlled
- Pupils are not allowed to access personal email using school Internet facilities

***Chat, discussion and social networking sites***

These popular forms of electronic communication are used more and more by pupils out of school, and can also contribute to learning across a range of curriculum areas.
Online chat rooms, discussion forums and social networking sites can present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

Pupils may become exposed to inappropriate material of a sexual, violent or extremist nature, and may come into contact with people who seek to 'groom' young people and encourage inappropriate, dangerous and in some cases illegal activities and behaviours.

We use the resources, guidelines and materials offered by Kidsmart, Think U Know and Childnet  as outlined above in the Safe Use of the Internet section to teach children how to use chat rooms and social networking and messaging tools safely and appropriately.

As part of other learning in Citizenship and PSHE children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced, inaccurate or that promote an extreme lifestyle or point of view.
The school uses DfE guidelines and LA resources to support this – eg the Tower Hamlets PREVENT team.

Pupils may take part in discussion forums or post messages on bulletin boards that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

- Pupils are not allowed to use public chat rooms, message boards or social networking sites in school, and are reminded that such sites usually have age restrictions – 13 and older in most cases.

**COVID19 - School Safeguarding Policy - Addendum**

**Online safety in schools and colleges**

Clara Grant will continue to provide a safe environment, including online. This includes the use of an online filtering system.

Where students are using computers in school, appropriate supervision will be in place.

**Children and online safety away from school and college**

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the School code of conduct.

Clara Grant will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

The Clara Grant school does not encourage staff to deliver live online lessons or sessions without another member of staff being present below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No 1:1s, groups only unless permission to record is obtained. The live session should be recorded so that if any issues were to arise, the video can be reviewed before being deleted
- Families may have many children who need to be online so maybe unable to see the session/lesson you deliver unless the sessions are staggered or there is more than one device
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used by staff should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by The Tower Trust to communicate with pupils
- Staff should record the attendance at any sessions held.

### ***Google Meet and Safeguarding***

As a result of COVID 19, the use of video conferencing tools like Google Meet or zoom is part of the 'new normal'.  At Clara Grant, we have enabled Google Meet for all teachers and students and Zoom for use with Class Dojo but with a few caveats to help safeguard the children.  No student is allowed to host a meeting, only an adult/teacher would be able to host a meeting.

The host can allow an external participant to join a meeting, and this feature is important to enable teachers to host meetings with parents.  It is the responsibility of the host (teacher) to carry out due diligence before sending a meeting link or a meet code to an external participant; Parents joining a meet while children are on the same meet, is one such example.  This is strictly prohibited and against our safeguarding policy.  When you start a meeting, **<u>it is very important that you give your meeting a code.</u>**  This will allow your students to join only if you are present at the meeting.  If you don't provide your meeting with a name, your students will be able to join the meeting whether you are present or not. After the meeting the meet code should be disabled.

## 9. Cyberbullying

***Online bullying and harassment***
Online bullying and harassment via Instant messaging, mobile phone texting, email and chat rooms are potential problems that can have a serious effect on pupils. Our school has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

- No access to public chat-rooms, Instant Messaging services and bulletin boards.
- Pupil email is monitored and checked for inappropriate use.
- Pupils are taught how to use the Internet safely and responsibly, and are given access to guidance and support resources from a variety of sources.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyberbullying are dealt with in accordance with our **Anti-Bullying Policy**.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

***Internet-enabled mobile phones and handheld devices***
Young people now have access to sophisticated internet-enabled devices such as SMART mobile phones, tablets and music players.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or weblog.

- *Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the Reception for pupils who need them on their journey to school.*
- *Pupils are not allowed to take photographs using a camera phone or other camera of people or property on school premises unless given permission by a member of school staff.*
- ***Pupils must under no circumstances upload pictures taken at school to a public website***

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc and how the data protection and privacy laws apply.

## 10. Contact details and privacy

As specified elsewhere in this policy, pupil’s personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

Pupils are taught that sharing this information with others can be dangerous

***School and pupil websites – pictures and pupil input***

- As part of the Computing and wider curriculum, pupils may be involved in evaluating and designing web pages and web-based resources.
- Any work that is published on a public website and attributed to members of our school community will reflect our school, and will therefore be carefully checked for mistakes, inaccuracies and inappropriate content.
- Pupils may design and create personal web pages. These pages will generally only be made available to other school users, or as part of a password protected network such as the LGfL.
- Where pupil websites are published on the wider Internet, perhaps as part of a project with another school, organisation etc, then identifying information will be removed, and images restricted

## 11. Deliberate misuse of the internet facilities by pupils

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

***Sanctions will include:***

**Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)**

- Initial warning from class teacher
- Banning from out of school hours Internet facilities
- Letter to parent/carer
- Report to Head

**Offensive material (**e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to Head teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement
- Removal of Out of School Hours access to Internet
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

***How will complaints regarding e safety be handled?***

It is the duty of the school to ensure that every child in our care is **safe**, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings.

International scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- All incidents will be recorded
- Interview/counselling by class teacher, Senior Management Team, e safety Coordinator and Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Our e safety Coordinator acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

## 12. Rules for responsible ICT use for KS1 pupils Keep safe: Keep SMART

- I will always ask before I use ICT equipment like a computer, laptop or camera
- I will make sure an adult is with me when I use the Internet
- I will ask an adult if I get lost or don't know what to do
- If I see anything I don't like or understand, I will tell an adult
- I will use school ICT equipment sensibly and carefully
- I will never give out personal information like my name and address to someone on the Internet
- I will not talk to strangers on the Internet

**I agree to try and follow all these rules to keep me safe online**

| | |
|---|---|
| **Class Name:** | **Date:** |
| **Signatures:** | |

# 13. Rules for responsible ICT use for KS2 pupils Keep safe: Keep SMART

*These rules will keep me safe and help me to be fair to others.*

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only email people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file unless directed by an adult in the class.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

**I have read and understand these rules and agree with them.**

| | |
|---|---|
| **Class Name:** | **Date:** |
| **Signatures:** | |

# 14. Online Letter to parents

**RE: Online safety**

Dear parent,

Due to increased access to numerous different technology platforms, many children are at a greater risk of online grooming, cyber bullying and exposure to inappropriate or illegal content online. At Clara Grant Primary School, we believe that promoting online safety plays a critical role in protecting our pupils online. We are writing to you today as we believe it is important for us to work in partnership with you as a parent, to keep pupils safe online.

Our online safety measures enable us to provide an environment for all our pupils to thrive, grow and learn, whilst staying safe online. We put these measures in place through policies and security provisions which safeguard pupils against unsuitable content and contact, and ensure they maintain appropriate conduct.

These policies include our Child Protection and Safeguarding Policy, Online Safety Policy, Acceptable Use Agreement and staff and pupil codes of conduct, which outline the proper use of technology for both pupils and staff. If any incidents breaching these policies occur, they are logged and managed in accordance with the relevant policy.

We have a number of procedures in place to ensure children cannot access unsuitable websites when using school technology, including software which blocks all websites with adult, violent or age-inappropriate content. Social media sites are also blocked, unless they are school pages used within lessons and under supervision. Online safety is taught to all pupils during IT lessons and staff are required to undertake online safety training to update their knowledge.

There are many ways you can help minimise the risks associated with children being online and increase online safety in your home – the list below provides ideas for some of the ways you can do this.

- Only give your children devices or access to devices that you feel comfortable with, and not as a result of peer-pressure deriving from their classmates/friends who are also using those devices. e.g. gaming systems and mobile phones at a young age.

- Talk to your children about why it is important to stay safe online. Explain that whilst the internet is a fun, exciting and knowledge-rich tool, it is also a place where people may wish to bring them into dangerous activities or expose them to unpleasant material. It is important to be clear that you are not saying your child may never use the internet again, or that everything on it is harmful – it is about teaching them to have a greater awareness and to be able to manage and report any risks.
- Discuss rules for being online and draw them up together, including which sites, games, etc., are acceptable. If certain games are off-limits, try to explain why, for example, because of excessive violence. If your child uses online gaming, consider setting rules, such as only talking to others in the same age range and having the conversation on speaker, rather than headphones, so you can monitor it.
- Discuss what information should be private and what is ok to share; for example, addresses, names of schools, and names should never be given out to strangers online, as this could allow them to identify where your child goes to school or lives.

- Keep an open dialogue with your child – letting them know they can always talk to you about anything that has made them feel uncomfortable online is key to keeping them safe.
- Ensure all devices used by your child are kept in a communal space, or a space where they can be supervised whilst using their devices.
- If your child uses a mobile device then set parental controls – do this as a dialogue with your child so they are aware of what they are not allowed to view; however, do not rely on parental controls on devices, as they are not always 100 percent effective and many children know how to bypass them.
- Make sure your child knows how to report or 'block' unsuitable content, messages or people online – show them how to block on the websites or games they frequently use and explain that they can always tell you, a teacher or another adult if they experience anything which makes them feel uncomfortable.

If you would like to discuss the matter of online safety in greater depth, please contact our Designated Safeguarding Lead, Karen Symons.

For more information on ensuring your child's safety online, you can visit our school website: http://www.claragrant.towerhamlets.sch.uk/e-safety.html.

Yours sincerely,

## 15. Use of the Internet and ICT resources by school staff

### *The Internet*

Our school understands that the Internet is a valuable resource for school staff. It provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in discussion.

It also provides an efficient way to access information from the DoE and other government agencies that will help staff to keep abreast of national and local developments, and engage in CPD.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

### *Internet Availability*

To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use. The school also provides an LGfL user account that gives further access to specific resources and online tools.

### *ICT Equipment and Resources*

The school also offers staff and pupils access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

### *Professional use*

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.

Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the Computing Coordinator

### *Personal use of the Internet and ICT resources*

We recognise that staff may occasionally find it useful to use the Internet at work for personal purposes. They may also wish to borrow school ICT equipment for personal use, either in or out of school.

Some equipment is available for loan to staff, with permission from the Computing Coordinator and Headteacher. The appropriate forms and agreements must be signed.

However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below.

### *Email*
We recognise that email is a useful and efficient professional communication tool. To facilitate this, staff members will be given a school email address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.

Staff are reminded that using this email address means that they are representing the school, and all communications must reflect this.

### *Online discussion groups, bulletin boards and forums, online chat and messaging*
We realise that a growing number of educationalists and education groups use discussion groups, online chat forums and bulletin boards to share good practice and disseminate information and resources.

The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, although staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

### *Social Networking*
The school appreciates that many staff will use social networking sites and tools. The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements.

### *Data Protection and Copyright*
The school has a data protection policy in place – please see separate documentation for more details.

Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.

Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

## 16. School Staff Agreement Form

**This document covers the use of school digital technologies and networks in and out of school.**

***Access***

- I will obtain the appropriate log on details and passwords from the ICT Co-ordinator
- I will not reveal my password(s) to anyone other than the persons responsible for managing the network
- If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me
- I will not allow unauthorised individuals to access school ICT systems or resources
- I will only use a personal device that has been sanctioned by the school and is fully protected with the school Sophos antivirus and antimalware software. Email abibi@claragrant.towerhamlets.sch.uk for further details.

***Appropriate Use***

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- I will ensure that my activities on social media do not breach professional conduct standards (see Teacher Standards – Professional Conduct section)
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending email, contributing to online discussion or posting to public websites using school facilities
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

***Professional Conduct***

- I will not engage in any online activity that may compromise my professional responsibilities
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role
- I will never include pupils or former pupils as part of a non-professional social network or group
- I will ensure that I represent the school in a professional and appropriate way when sending email, contributing to online discussion or posting to public websites using school facilities
- I will not browse, download or send material that could be considered offensive to colleagues
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact

***Email***

- I will only use the approved, secure email system for any school business or communication with parents (currently: LGfL Staff Mail)
- I will not communicate with pupils by email unless using approved school email accounts as part of approved school work

***Photographs and Video***

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance).

***Personal Use***

- I understand that I may use Internet facilities for personal use at lunchtimes, break times and before and after school, where computers are available and not being used for educational purposes.
- I understand that I may access private email accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the forwarding of email chain letters, inappropriate 'jokes' etc is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or bulletin boards, chat rooms or Instant Messaging.

***Use of School Equipment out of school***

- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue and Customs.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and will return it when requested to be updated by the school technician
- I will not connect a computer, laptop or other device to the network that does not have up-to-date anti-virus software.

***Teaching and Learning***

- I will always actively supervise, or arrange for suitable adult supervision of pupils that I have directed or allowed to use the Internet.
- I will embed the school's e safety curriculum into my teaching, using agreed resources and materials.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a classroom with Internet access.

***Copyright***

- I will not publish or distribute work that is protected by copyright.
- I will teach pupils to reference online resources when they use them in a report or publication.

***Data protection***

- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students working at the school.
- I will keep my School Google Drive password safe at all times and if breached, I will request a new password from the Connetix helpdesk.
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

- I will respect the privacy of other users' data, and will never enter the file areas of other staff without their express permission.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

**User Signature**

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e safety policies.
- I wish to have an email account, be connected to the Internet via the school network and be able to use the school's ICT resources and systems.

## 17. Staff Declaration Form

All members of staff are required to sign this form.

- By signing this form, you are declaring that you have read, understood and agreed to the terms of the School Staff Agreement Form. You should read and sign the declaration below before returning it to the school office.
- Members of staff are required to re-sign this declaration form if changes are made to the policy.
- I have read name of school's School Staff Agreement Form and understand that:
- School equipment must not be used for the fulfilment of another job or for personal use, unless specifically authorised by the headteacher.
- Illegal, inappropriate or unacceptable use of school or personal equipment will result in disciplinary action.
- Passwords must not be shared and access to the school's computer systems must be kept confidential.
- I must act in accordance with this policy at all times.

| | |
|---|---|
| **Name of staff:** | |
| **Job title:** | |
| **Signed:** | |
| **ICT technician signed:** | |
| **Headteacher signed:** | |
| **Date signed:** | |

## 18. Data Protection Policy

Our school is aware of the data protection law as it affects our use of the Internet, both in administration and teaching and learning.

We adhere to the LA Guidelines on Data protection.

Staff and pupils understand the legal and disciplinary implications of using the Internet at school for illegal purposes.

Where appropriate, the police and other relevant authorities will be involved in cases of deliberate misuse or abuse of the Internet by members of the school community using the connection provided by the school.

## 19. Staff Laptop and ICT Equipment Loans

Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this e safety Policy.

This must be the case wherever the laptop, computer or other such device is being used as it remains the property of Clara Grant Primary School at all times.

Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

Staff must sign the 'Staff Laptop and Computer Loans Agreement before taking the equipment away from the school premises.

## 20. Staff Laptop and ICT Equipment Loan Agreement

**I have borrowed a school laptop to use out of school in agreement with both Head Teacher and the Computing Coordinator**

Make: ________________________________

Model: ________________________________

Serial number: ________________________________

**It is understood that I will return the equipment to school if requested to do so by either the Head Teacher or the Computing Coordinator**
I undertake to take proper care of the equipment whilst in my possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. I agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, I will replace or arrange for the repair of the equipment at my own expense.

I will use the equipment in accordance with the schools Acceptable Use of the Internet and Related Technologies (IAU Policy) and ICT Policy.

**I agree to the above conditions:**

(Signature) _____________________________

(Print name) ______________________ Date:___________

**Returned:** ________________________ Date:___________