



Online Safety Policy

This policy should be read in line with:

The Acceptable Use Policy

The Anti-Bullying Policy


Computing curriculum Policy

Software Procedure

Remote learning policy

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	Sue Rademacher Ankita Banerjee Samira Assou
	Online-safety lead	Garsa Hakmal
	Online-safety / safeguarding link governor	Jennifer Flanigan Tambra Wheeler
	PSHE/RSHE lead	Lidia Cernat
	Date this policy was reviewed and by whom (Garsa Hakmal)	March 2023
	Date of next review and by whom	March 2025

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE), 'Teaching Online Safety in Schools' 2023 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside your school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These

three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

How will this policy be communicated?

It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Contents

Introduction	1
Key people / dates	1
What is this policy?	1
What are the main online safety risks today?	1
How will this policy be communicated?	2
Contents	2
Introduction.....	3
Scope.....	4
Roles and responsibilities	4
Headteacher/Principal	4
Online Safety Lead	5
All staff	6
Computing Lead	Error! Bookmark not defined. 7
Subject / aspect leaders.....	7
Network Manager/technician	8
Pupils.....	8

Parents/carers.....	9
Upskirting.....	9
Bullying.....	9
Social media	10
Appropriate filtering and monitoring	10
Email.....	11
Online safety in the curriculum.....	13
Online Behaviour.....	14
Online safety skills development for staff.....	14
Incident reporting, online safety incident log & infringements incident reporting	14
Internet access.....	15
infrastructure.....	15
Parental involvement.....	15
Passwords and passwords security.....	16
Safe use of images.....	17
Consent of adults who work at the school.....	17
Publishing pupils work.....	17
Storage of images	18
Mobile Devices.....	18
Computer Viruses.....	20
Review Procedure.....	20
Appendix 1: Actions where there are concerns about a child	
Appendix 2: Online _Safety References	
Appendix 3: Mobile phoned and media devices student agreement.	
Appendix 4: Staff and Governor Acceptable Use Agreement / Code of Conduct	
Appendix 5: Student Acceptable Use Agreement / Online Safety Rules	
Appendix 6: Staff Mobile Phone Declaration	
Appendix 7: Computer Gaming	
Appendix 8: Protocol for Staff Using Virtual Teaching Software	
Appendix 9: Rules for lessons online	
<u>Appendix 10: Expectations for safe home learning for Secondary</u>	

Introduction

- At John Chilton School we set out expectations for all members of staff' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
 - for the protection and benefit of the children and young people in their care, and
 - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
 - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).
- Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.
- Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school such as PCs, laptops, iPads, whiteboards, digital video equipment, etc; and technologies owned by pupils and staff, but brought onto school premises such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.

Scope

This policy applies to all members of the John Chilton School community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirement

Key responsibilities

- Ensure "An effective approach to online safety [that] empowers the school to protect and educate the whole school in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees
- Receive regular updates in online safety issues and legislation
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues, review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff use LGfL filtering,
- Facilitate training and advice for all staff:
 - all staff must read KCSIE P
 - cascade knowledge of risks and opportunities throughout the organisation

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Keeping Children Safe in Education (Read and follow this policy in conjunction with the school's main safeguarding policy)
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself

- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Computing Lead: Garsa Hakmal

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician

Key responsibilities:

- As listed in the 'all staff' section, plus:
- 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
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- 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 and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying

Social media

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and

pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

We teach our pupils to use social networking sites responsibly both outside and within an educational context. It is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavours to deny access to social networking sites to pupils within school
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online
- Our pupils are asked to report any incidents of bullying to the school

Appropriate filtering and monitoring

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

E-Mail

- Pupils at this school use the LondonMail / PupilMail system from LGfL for all school emails
- Staff at this school use the StaffMail system for all school emails

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

The use of e-mail within the school is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'. ICT Entry Pathways and ICT Ed-Excel assessment criteria require pupils to send and receive emails.

Managing e-Mail

The school gives all staff their own e-mail account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
 - Delete all e-mails of short-term value
 - All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission
 - Only send emails to the intended recipients – do not "piggy back" off another email which was sent to non-intended recipients.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail
- Staff must inform the Headteacher/ line manager if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the computing Scheme of Work
- However you access your school e-mail (whether directly, through webmail or on non-school hardware) all the school e-mail policies apply
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section E-mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- Never open attachments from an untrusted source; Consult a member of the ICT staff first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed without prior authorisation from the E Safety Coordinator.

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail - e-mailing confidential data is not recommended and should be avoided where possible
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted
- Where your conclusion is that e-mail must be used to transmit such data:
 - Obtain express consent from your manager to provide the information by e-mail
 - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
 - Verify the details, including accurate e-mail address, of any intended recipient of the information
 - Verify (by phoning) the details of a request or before responding to e-mail requests for information
 - Do not copy or forward the e-mail to any more recipients than is absolutely necessary

- If possible, send the email using a secure means (e.g. Egress – this is available through the school office)
- Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)

Online Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. E-Safety is embedded within our curriculum. Teaching is built into existing lessons across the curriculum, covered within specific online safety lessons. We continually look for new opportunities to promote e-Safety in an age appropriate and meaningful way:

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum and an annual Safer Internet Day set of activities.
- Pupils are taught about personal and private information and the impact of this on the internet
- Pupils are aware of the impact of Cyber bullying including mobile phones, iPads, tablets and other devices and know how to seek help if they are affected by any form of online bullying.
- Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.
- Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Child line or CEOP
- All pupils are reminded of Student Acceptable Use Agreement/ Online Safety Rules
- it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- At John Chilton School we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety)

Online Behaviour

Part of the online safety lessons, pupils are taught to understand what acceptable and unacceptable online behaviour looks like and that the same standard behaviour and honesty apply online and offline.

Pupils are made aware on how to identify possible online risks and make informed decisions about how to act.

Pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

Online safety- Remote learning (see appendix 9, 10, 11)

At John Chilton we understand the need to continue to provide quality learning and education opportunities, including periods of lock and national lock-down for class groups, individuals or whole school.

- All students will have access to remote education as soon as reasonably practicable, using Google Classroom and Zoom for online lessons
- Our staff only use school-registered accounts, never personal ones
- Admin settings audited t (who can chat? who can start a stream?, who can join?)
- Check the link in an, incognito tab to make sure it is not public for the whole world!

At John Chilton School we encourage parents and carers to provide age-appropriate supervision for the internet use of the children and young people in their care.

There is regular and appropriate parental engagement in online safety,

Online Safety Skills Development for Staff

- Our staff receive regular information and training on e-Safety issues in the form of feedback on training received from the computing coordinator INSET on e-Safety
- All staff undergo safeguarding and child protection training including online safety. Training is regularly updated
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas

Incident Reporting, e-Safety Incident Log & Infringements Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's e-Safety Co-ordinator.

Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner (Sue Radmacher). (see appendix 1)

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **London Grid for Learning** (LGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Staff recommend and use internet sites in the following way:

- Checking on pupils during lessons
- Raw image searches are filtered through our system and by individual user name
- Safe and checked sites are recommended for home learning activities
- The use of individual log-ins for staff and pupils
- Using LGfL pre-programmed sites to minimise risk

Infrastructure

- Ealing Local Authority has a monitoring solution via the London Grid for Learning where web-based activity is monitored and recorded. School internet access is controlled through the LGfL's web filtering service.
- Our school also employs some additional web filtering which is the responsibility of the contracted Network Management team. John Chilton School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the network management team, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We

communicate with parents/ carers concerning e-Safety and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school
- We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to Online safety where appropriate

In school we have 'appropriate filtering' but at home many parents will not be using **parental controls**.

- Parental guides sent home to support parents with safe settings, controls and monitoring.
- Introduce **child-safe search engines** e.g. [swiggle.org.uk](https://www.swiggle.org.uk) and **YouTube Kids** instead of YouTube.
- Parents Online safety workshops throughout the year to provide them with update information on apps, games software they need to be aware of.
- Letters sent home making parents aware of new apps and games their children might be accessing. **(see appendix 8)**
- Online safety information available for parents on school website.
- Parents informed and supported if their child is found to be having online access that raises concerns **(see exemplar letter in appendix 12)**

Passwords and Password Security

Passwords

- Always use your own personal password to access your LGfl and e-mail account
- Use staff username and password to access the network. Staff must log off on a computer used to access the network.
- User ID and passwords for staff and pupils who have left the School are removed from the system within 2 weeks
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy and Data Security
- In our school, all ICT password policies are the responsibility of the Network Manager and all staff and pupils are expected to comply with the policies at all times

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the pupil's device

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file

Publishing Pupil's Images and Work

On a pupil's entry to the school, parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- general media appearances, require local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published

We will be using your child's images/videos/class work;

- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- by posting student work on the Internet (without using pupils' names and images).
- In recorded/ transmitted videos for curriculum purposes.

Only the Headteacher has authority to grant permission to upload to the site.

This consent form is considered valid for the entire period that the child attends this school

unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. You can withdraw permission at any time.

Storage of Images

- Images/ films of children are stored on the school's network and on teachers 'laptops for school related work
- Pupils staff and parents are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network

School ICT Equipment including Portable & Mobile ICT Equipment & Removable Media

School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Visitors will be directed to the wireless ICT Facilities available
- Ensure that all ICT equipment that you use is kept physically secure
- It is imperative that you save your data on a frequent basis to the school's network drive.
- You are responsible for the backup and restoration of any of your data that is not held on the school's network drive
- Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted and no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, return all ICT equipment to your Manager.
- All ICT equipment allocated to staff must be authorised. The Network Manager is responsible for:
 - o maintaining control of the allocation and transfer of equipment
 - o recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop.
- Equipment must be kept physically secure at all times in accordance with this policy to be covered for insurance purposes.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised the leadership team and undertaken by the network management team
- Portable equipment must be transported in its protective case if supplied.

Personal Mobile Devices (including phones) - Staff

- The school allows staff to bring in personal mobile phones and devices for their own use. Staff should only use their phone outside of working hours or during break times unless express permission has been sought from the Headteacher.
- Only under exceptional and necessary circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. If it has been necessary to make a call in this way, the E-Safety Co-ordinator must be informed.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

Personal Mobile Devices (including phones) - Pupils

- Pupils are not allowed to bring personal mobile devices/phones to school unless prior permission is sought. At all times during the school day, the device must be switched off.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Pupils may not make any image or sound recordings on these devices of any member of the school community
- Pupils bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- All pupils must sign the mobile phone and social media agreement. (See appendix 4)

School Provided Mobile Devices (including phones) - Staff

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and tablets for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school. Where this is not possible or practical, the Headteacher should be informed.
- All staff must sign the mobile phone agreement. (See appendix 8)

School Provided Mobile Devices (including phones) - Pupils

- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as laptops and tablets for offsite visits and trips, only these devices should be used

Removable Media

- Only use recommended removable media
- Store all removable media securely
- Removable media must be disposed of securely by the Network Manager

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB stick, CD) must be checked for any viruses using school provided anti-virus software before using them
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact a member of the ICT staff. The ICT staff member will advise you what actions to take and be responsible for advising others that need to know

Review Procedure

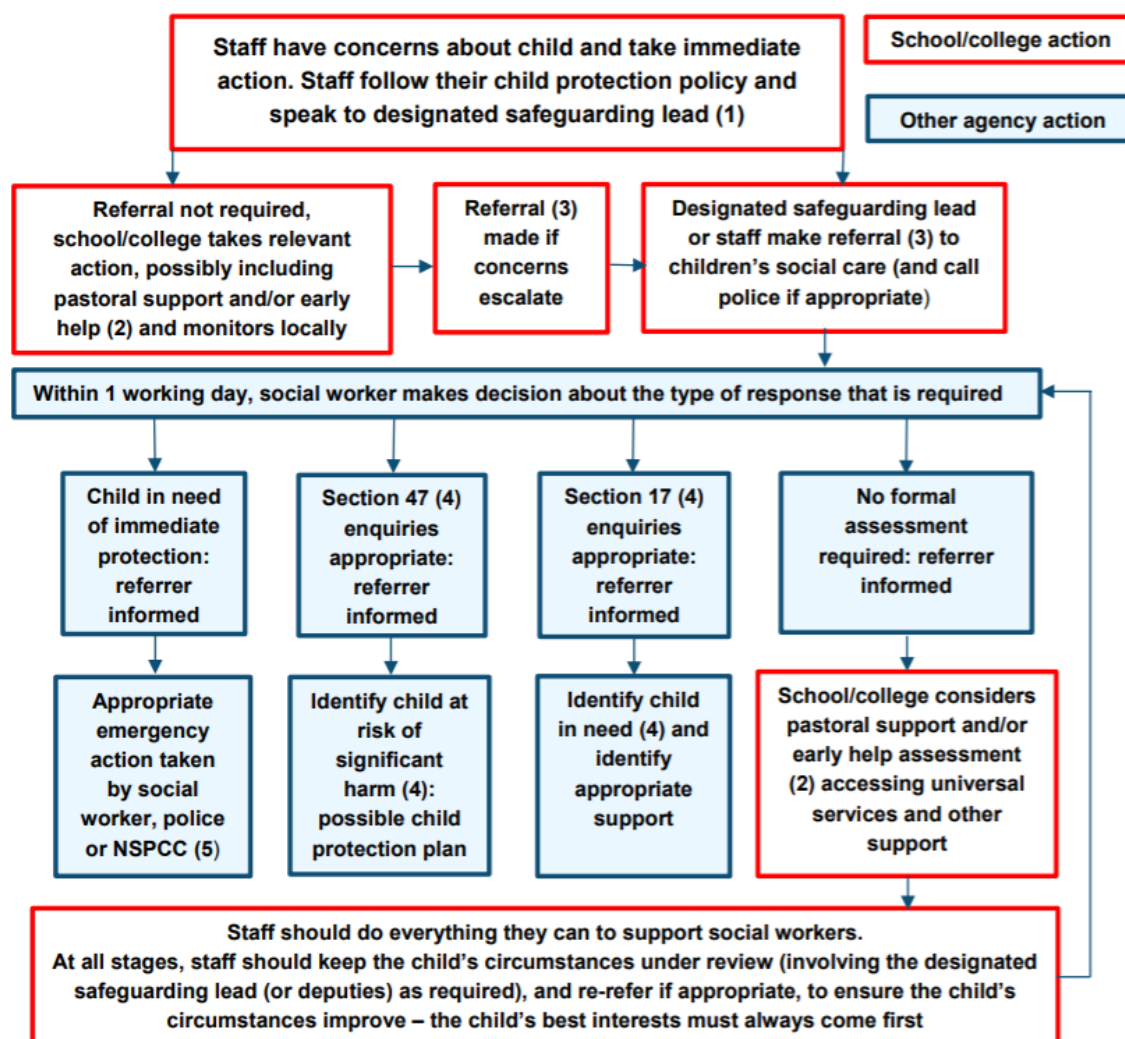
There will be an on-going opportunity for staff to discuss with the e-Safety coordinator any issue of e-Safety that concerns them

This policy will be reviewed every two years and consideration given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Updated March 2023
Garsa Hakmal

Actions where there are concerns about a child



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of [Working Together to Safeguard Children](#) provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of [Working Together to Safeguard Children](#).

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of [Working Together to Safeguard Children](#).

(5) This could include applying for an Emergency Protection Order (EPO).

Online **-Safety References**

Particularly for Parents and Children

National Action for Children (NCH) www.nchafc.org.uk/itok/
Parents' Guide on Internet usage

Bullying Online www.bullying.co.uk
Advice for children, parents and schools

FKBKO - For Kids By Kids Online www.fkbko.co.uk
Excellent Internet savvy for kids; KS1 to KS3

Parents Information Network (PIN) www.pin.org.uk
Comprehensive guidelines on Internet safety

Parents Online www.parentsonline.gov.uk/2003/parents/safety/index.html
Interactive learning and safety advice,
excellent presentation for parents.

Kidsmart www.kidsmart.org.uk
An Internet safety site from Childnet,
with low-cost leaflets for parents.

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining
internet dangers and how to stay in control.

Family Guide Book (DfE recommended) www.familyguidebook.com
Information for parents, teachers and pupils

NCH Action for Children www.nchafc.org.uk
Expert advice for children, young people and parents.

Safekids www.safekids.com
Family guide to making Internet safe, fun and
productive

Childnet International www.childnet.com/resources/esafety-and-computing
Information for parents, teachers and pupils



MOBILE PHONES & MEDIA DEVICES STUDENT AGREEMENT

We recognise that mobile phones and media devices are part of everyday life for many young people and that they can play an important role in helping them feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying and intimidating others.

We allow these items to be brought to school provided that the student agrees to uphold the rules below; otherwise, phones and media devices are forbidden.

Students are responsible for the safe-keeping of their phones and media devices in school unless handed in to the school office for safekeeping during the day.

Rules that apply if phones or media devices are brought to school

- Phones and media devices must be switched off and placed in a school bag or in the school office during the whole of the school day.
- Phones and media devices must NEVER be used during the school day. This includes taking pictures, making calls, sending texts or listening to music at any time during the school day including during break and lunchtime.
- Phones and media devices must NEVER be used in lessons or during lesson changeover. Headphones must also be put away at the start of the school day.
- The contents of phones and media devices must be suitable for viewing at school; there must be nothing on them that students would be embarrassed for staff in the school to see. Bringing a phone or media device to school means accepting that staff may ask to see the contents should there be any concerns.
- Phones and media devices must NEVER be used for any act of unkindness.
- If any of the rules are broken, the school may confiscate the device and require the student's parent/carer to collect it.

Student's Name: _____

Signed _____ Date: _____



Staff and Governor Acceptable Use Agreement / Code of Conduct

Appendix 4

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct.

I have read the e-safety policy and am in agreement with my designated responsibilities

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature Date

Full Name(printed) Job title

I take this opportunity to give Permission for the school to use images of myself appropriately in school publications and on the school website.

John Chilton School Online Safety Policy March 2023

Signature..... Date



Student Acceptable Use Agreement / Online Safety Rules

Appendix 5

- I will only use the school's email / Internet / Intranet and any related technologies for school purposes.
- I will not disclose my password provided to me by the school.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address to anyone.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find inappropriate content I will tell my teacher immediately.
- I will tell an adult if we see anything we are uncomfortable with.
- I will only send e-mails that are polite and friendly.
- I will never arrange to meet anyone we don't know.
- I will not use Internet chat rooms.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.



Staff Mobile Phone Declaration

Appendix 7

The aim of the Mobile Phone Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice and to ensure that members of staff are fully aware of their professional responsibilities.

The school allows staff to bring in personal mobile phones and devices for their own use.

- Staff should only use their phone outside of working hours or during break times. Only under exceptional and necessary circumstances does the school allow a member of staff to use their personal device. If it has been necessary to make a call in this way, a Headteacher or a member of SLT must be informed and permission must be sought.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device
- Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office
- Staff are not permitted to use their own personal phones for contacting children, young people and their families within or outside of the setting. If staff are out on a school trip they need to take the school mobile phone for emergency use such as contacting parents or the school.
- Staff should have their phones on silent or switched off and out of sight (eg in a drawer, handbag) during class time.
- Mobile phones should not be used in a space where children are present (eg classroom, -corridor, playground).
- Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras, iPads or school phones.
- Staff should report any usage of mobile devices that causes them concern to the ; Headteacher.

Name: _____

Signed: _____ Date: _____


COMPUTER GAMING – essential E-Safety information **for parents**

Lots of pupils enjoy playing games on their game console; however there are some games that pupils are playing that are not appropriate for their age.

The games that pupils and parents most frequently mention are **Grand Theft Auto 5** and **Call of Duty**. Both of these games are given a PEGI rating of 18. All games are given PEGI ratings.

What is a PEGI rating ?

Age ratings are systems used to ensure that entertainment content, such as films, videos, DVDs, and computer games, are clearly labelled by age according to the content they contain. Age ratings provide guidance to consumers (particularly parents) to help them decide whether or not to buy a particular product.

Why are games given age ratings of  ?

The rating will be accompanied by a description of why the game has been rated.

The content of this game is suitable for persons aged 18 years and over only. It contains:
Extreme violence – Multiple, motiveless killing – Violence towards defenceless people – Strong language This game allows the player to interact with other players ONLINE

The graphics in these games are extremely realistic. They are very much like watching a movie. The content of such games typically includes:

- Continuous swearing
- Extreme violence being depicted against defenceless people including prostitutes – e.g. someone's head being stamped on; people being stabbed
- Sexualised content and demeaning images of women– people having sex; picking up prostitutes; assaulting lap dancers etc
- Drug taking

E-Safety is an important part of keeping children safe at John Chilton School.

The school's message is very clear: These games are NOT appropriate for Primary and secondary School aged children. Young children are very impressionable. They do not have the maturity or experience of life with which to interpret such degrading content. Their values are being influenced for the worse. There is an added danger of children being groomed by online contacts pretending to be children.

Whilst the school tries to offer helpful advice to parents, we obviously cannot prescribe what parents allow their children to do at home. However, children tend to imitate what they see and

hear. Children coming into school and swearing, using degrading language or acting out offensive things they have seen, will find themselves in trouble.

We talk a lot to the children in school, and we know that some children are currently allowed to play these games. We also know that the majority of parents do not let their children play such games. It has always been the case (even when we were young!) that children use pester power to say that ALL MY FRIENDS ARE ALLOWED TO ... [stay up late; wear certain types of clothes etc] ... IT'S SO UNFAIR. Sensible parenting is about making the right choices even when children don't agree.

We wouldn't let our children go to a friend's house if we didn't trust that they would look after them. Have a chat with the other parents, they will probably share your opinion. Just as importantly, have a chat with your child; explain why you don't let them play these games at home and why you do not want them to go behind your back. In this day of 'internet everywhere', educating your child is one of the best ways of helping to safeguard them.

For signposting to further information and advice, please go to the section on our school website:

<http://www.john-chilton.ealing.sch.uk/E> -



10

Appendix 9

Protocol for Staff Using Virtual Teaching Software



High Expectations:

Ensure that:

- there is a minimum of at least 2 online sessions each day.
- work is always completed when expected and follow this up if not, let SLT know of any concerns
- pupils attend every lesson follow up to find out reasons behind absences
- pupils attend all lessons on time
- Pupils behave appropriately
- anyone to one virtual sessions are carried out in classroom space with other colleagues in room and aware they are taking place

Technical safety and protocol

Ensure that:

- attendance is logged each day and inform SLT of any concerns
- pupils have their cameras on in lessons
- pupils are not on mute unless agreed otherwise
- teacher is first to arrive and last to leave the virtual lesson
- pupils use their own devices
- pupils use their own logins
- Not sharing personal data over classrooms
- Limiting student access to what is necessary

Settings and Links

Ensure that:

- restrictions are correct for pupils' settings (so they can't share screens or take over the lesson, etc- chat to Rob and Garsa if unsure)
- the link to lesson is at top of communication stream (it can be 'set' in 'options' to stream from the top)
- the link is scheduled to appear 10 minutes before lesson (this can be 'set' in 'options')
- staff use same link each time, no need for different one
- Sending invites out to only attendees.
- Data sharing – Personal data will not be shared.
- Limiting student access to Zoom.
- Ensuring there is a pin code before entering the call.
- Ensuring the host has to "admit" the individual into the call.
- Users must change their passwords regularly.
- Users passwords are required to have a combination of upper and lower-case letters, numbers and symbols.
- To remind user's not to display personal information in the background to the call.
- Only worksheets and other educational materials

Safeguarding

Inform SLT of any safeguarding concerns in usual ways

Housekeeping (ask Garsa)

Delete work from Google classrooms/ forums regularly - this is the responsibility of teachers

Delete work for any pupil who leaves the school- this is the responsibility of teachers

Staff Absence

If absent, ensure class and parents know this by writing message on stream, but support staff still available to help cover teacher with virtual lesson where possible

Support staff to still log in for lesson and check any communication even if teacher is absent to say hello to pupils and check they received message the teacher was ill

Recording

Only film/ record pupil if needed for exams. In this case ensure videos are saved appropriately and with explicit written parental permission. Teacher ensures these are deleted afterwards.

Staff can film themselves if needed for modelling in lessons or if a known absence is planned for but teachers must delete as soon as possible once used. Any staff-filmed video must have been recorded in the appropriate and professional manner and setting in line with agreed expectations for conduct as set out in document:

E-Safety Acceptable Use Agreement for Staff and Governors (neutral background, professional language).

Edited March 2023

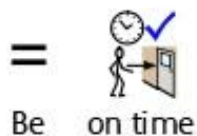
Garsa Hakmal



Rules for lessons online

1

1.



Be on time

2

2.



Have your equipment

3

3.



Sit up straight if you can

4

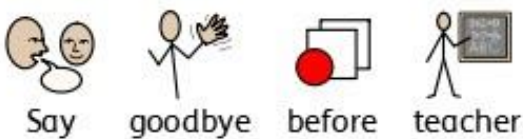
4.



Your camera must be on

5

5.



Say goodbye before teacher

6

6.



Log off

Expectations for safe home learning for Secondary

Pupils:

- Attend all virtual lessons and be on time
- Be appropriately dressed
- Sit at a table
- Be ready with pens, pencils, relevant activity, if applicable
- Log off promptly after each session (no private conversations)
- Make sure your camera is switched on for the lessons
- Put your microphone on mute when you are not talking if possible
- Use polite language (this includes household members in the background)

Parents/Carers:

- Try to choose a calm place for the pupil to access remote learning
- Ensure all devices are fully charged
- Try to ensure nothing can be seen in the camera except the pupil and their close environment (family members should avoid being in the background)
- Ensure other people in the household know a lesson is taking place to avoid interruptions
- Monitor the pupil's use of the internet at all times, especially if device belongs to the school
- Where possible, be alongside the pupil when sessions take place
- Ensure the pupil promptly logs off at the end of session
- Try to ensure the pupil isn't being distracted by toys during the session
- Help prepare the pupil to get ready for the lesson 5 minutes before they start, and be organised
- Set up a routine for learning where possible
- Let the class teacher know if a pupil will be unable to attend a remote session
- Contact the class teacher by email for any question or comment (unless a safeguarding concern – see below)

All:

- No recording, photographing, screenshots or streaming of sessions is permitted, unless you have the permission of all the participants (teachers will film for exam purposes only and delete afterwards)
- If you are concerned about any inappropriate content or any other safeguarding issue that arises during a session, please immediately contact the school's Designated Safeguarding Lead, Sue Rademacher. If you cannot reach the DSL quickly, you can also contact the NSPCC by telephoning 0808 800 5000 or emailing help@nspcc.org.uk.



Appendix 12

JOHN CHILTON SCHOOL
Bengarth Road
Northolt
Middlesex
UB5 5LD

Headteacher
Mrs Sue Rademacher

London Borough of Ealing

Dear Parents/Carers

Re: PlayStation 4 and Fortnite

I am sorry to have to write to you at this festive time regarding concerns. A number of pupils and parents have come to staff with worries about a few pupils use of PlayStation 4 and the game Fortnite. This game and system allow pupils to talk with each other outside school and this is causing some problems.

I am really pleased when pupils are able to spend their leisure times together and do not wish to stop healthy and safe friendships. Sadly, some of the language being used between some pupils is hurtful and in some cases racist and extreme. This then also affects the pupils' relationships in school and can lead to challenges.

One parent has linked headphones to their child's PlayStation and has been able to tell me the language involved. I urge you to please take the following steps over the holiday:

- Supervise the communication between your child and their peers on these games
- Make sure that your child is only talking with trusted friends
- Delete and block any friends that you think are rude or offensive in their speech or messages
- Make an appointment to speak with me or Mrs Hakmal about the situation if you are worried, we can help

I have spoken with all the pupils whose names have come up around this issue. I am confident that together we can ensure our children and young people are safe. Thank you for your support with this. Please contact me through the school office if you would like to talk further about this.

Yours sincerely

Sue Rademacher
Headteacher

Telephone: 020 8289 4790

E-Mail: admin@john-chilton.ealing.sch.uk

Website: www.john-chilton.ealing.sch.uk