EMPOWERING YOUNG PEOPLE TO TAKE ON THE WORLD

Online safety policy

Drafted By:	Stephanie Shaldas, Senior Leader and Designated Safeguarding Lead and Stephen Roworth, Network Manager
Date:	May 2021
Review date:	May 2022

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

Content

Appendices

1. Online Acceptable Use Agreement (Staff)
2. Online Acceptable Use Agreement (Volunteers, Visitors and Governors)
3. Online Acceptable Use Agreements (Students – adapted for phase)
4. Parental Acceptable Use Agreement including photo/video permission
5. Safeguarding protocol for virtual learning

Other related policies

- Preventing exposure to radicalisation policy (PREVENT)
- Safeguarding policy
- Preventing bullying policy
- School culture and behaviour for learning policy

1. Introduction and overview

1.1. Rationale and scope

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at School 21 with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

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

Content	Exposure to inappropriate content
	Lifestyle websites promoting harmful behaviours
	Hate content, including extremist material
	Inaccurate content validation
	False news and information
Contact	Grooming (e.g. for sexual exploitation and radicalisation)
	Online bullying in all forms
	Social or commercial identity theft, including passwords
Conduct	Aggressive behaviours such as online bullying
	Privacy issues, including disclosure of personal information
	Digital footprint and online reputation
	Health and wellbeing

	Sexting
	Copyright (little care or consideration for intellectual property)

Scope:

This policy applies to all members of School 21 community, including staff, students, volunteers, parents/carers, visitors, community users, who have access to and are users of school IT systems, both in and out of School 21.

1.2. Roles and responsibilities

Role	**Responsibilities**
Headteacher: Oli de Botton	● Must be adequately trained in offline and online safeguarding, in line with statutory guidance. ● To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. ● To take overall responsibility for online safety provision. ● To take overall responsibility for data management and information security (as the Senior Information Risk Officer) ensuring school's provision follows best practice in information handling. ● To ensure the school uses appropriate IT systems and services including, filtered internet service. ● To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. ● To be aware of procedures to be followed in the event of a serious online safety incident. ● Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised. ● To receive regular monitoring reports from the Online Safety Coordinator. ● To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures. ● To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety ● To ensure the school website includes relevant information. ● To ensure that the school is registered with the Information Commissioner (ICO).

Designated Safeguarding lead: Stephanie Shaldas	To liaise with the Child Protection Link Governor about online safety, and update the governing body through them on any issues that arise, and strategies used to tackle them.
Governors	● To ensure that the school has in place policies and practices to keep the children and staff safe online. ● To approve the Online Safety Policy and review the effectiveness of the policy. ● To support the school in encouraging parents and the wider community to become engaged in online safety activities. ● To assign the role of Child Protection Link Governor, who has the responsibility of liaising with the Online Safety Coordinator and feeding back to the rest of the governing body on online safety.
Heads of year/phase leaders	● To oversee the delivery of the online safety element of the pastoral curriculum, either through assemblies, coaching, talk time ● To address with students any alerts raised via Securly.
IT Manager and IT Team: Stephen Roworth	● To report online safety related issues that come to their attention to the Designated Safeguarding Lead. ● To manage the school's computer systems, ensuring school password policy is both rigorous and strictly adhered to. ● To ensure that robust systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) ● To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices ● To oversee the school's policy on web filtering, taking responsibility for it being applied and updated on a regular basis ● Helping shape and keeping 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. ● Ensuring that the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Designated Safeguarding Lead or Headteacher ● To ensure appropriate backup procedures and disaster recovery plans are in place. ● To keep up-to-date documentation of the school's online security and technical procedures.

Data and information (asset owners) managers (IAOs)	● To ensure that the data they manage is accurate and up-to-date ● Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
Teachers	● To embed online safety in the curriculum wherever appropriate. ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). ● To be vigilant in lessons and act immediately on any information related to the online safety of any child, adult or the school being compromised. ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. ● To adhere to safeguarding protocols when delivering online/ virtual lessons.
All staff, volunteers and contractors	● To read, understand, sign and adhere to the school staff Acceptable Use Agreement which can be found as an appendix to the Professional Code of Conduct and Online Acceptable Use Policy, and understand any updates annually. (The AUP is signed by new staff on induction.) ● To report any suspected misuse or problem to the Designated Safeguarding Lead. ● To maintain an awareness of current online safety issues and guidance. ● To model safe, responsible and professional behaviours in their own use of technology. ● At the end of the period of employment/volunteering to return all equipment or devices loaned by the school.
Parents and carers	● To read, understand and promote the school's Student Acceptable Use Agreement with their children, and realise that the school's online safety policy covers their child's actions out of school. ● To consult with the school if they have any concerns about their children's use of technology. ● To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images.
Students	● Read, understand, sign and adhere to the Student Acceptable Use Agreement annually.

	● To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school. ● To understand the importance of reporting abuse, misuse or access to inappropriate materials. ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology. ● To contribute to any surveys that gathers information on their online experiences.
External groups	● To read and sign the Acceptable Use Agreement: School Visitors prior to using technology or the Internet within school. ● To support the school in promoting online safety. ● To model safe, responsible and positive behaviours in their own use of technology.

1.3. Communication of policy

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

- Posted on the school website
- Linked to on The Source (School 21's internal communications portal)
- Included in the school induction pack for new staff.
- Regular updates and training on online safety for all staff as part of professional development days, the weekly CPD programme, and in briefing notices.
- Acceptable use agreements discussed with staff and pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, on entry to the school.

1.4. Handling incidents

The school will take all reasonable precautions to ensure online safety.

Staff and pupils are given information about infringements in use and possible sanctions. Online Safety Coordinator acts as first point of contact for any incident.

Any suspected online risk or infringement is reported to Online Safety Coordinator that day Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complainant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

1.5. Review and monitoring

The online safety policy is referenced within other school policies and will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

There is widespread ownership of the policy and it has been agreed by the senior leadership. The responsibility for signing it off has been delegated to the Headteacher and is monitored by the Executive Headteacher All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and curriculum

2.1. Student online safety curriculum

School 21:

- Has a commitment to covering online safety with every student, every year through the pastoral curriculum, tailoring the approach depending on the dangers which are current at the time and the age of the students.
- Covers online safety in other curriculum areas as relevant.
- Plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Reminds students about their responsibilities through the pupil Acceptable Use Agreement at least once a year.
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright.
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/ intellectual property rights.
- Ensure pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

2.2. Staff and governor training

School 21:

- Makes regular training available to staff on online safety issues and the school's online safety education program.
- Provides, as part of the induction process, all new staff and volunteers with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

2.3. Parent awareness and training

School 21

- Provides induction for parents which includes online safety.
- Runs a rolling programme of online safety advice, guidance and training for parents.

3. Expected conduct and incident management

3.1. Expected conduct

3.1.1. All users

In School 21, all users:

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

3.1.2. Staff, volunteers and contractors:

In School 21, all staff, volunteers and contractors:

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils.

3.1.3. Parents/Carers

In School 21, parents/carers:

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

3.2. Incident management

At School 21:

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions.
- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

- Support is actively sought from other agencies as needed (i.e. the local authority, Securly, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues.
- Monitoring and reporting of online safety incidents and the response to these takes place and contribute to developments in policy and practice in online safety within the school.
- Parents/carers are informed of online safety incidents involving young people for whom they are responsible.
- The Police are contacted if a member of staff or the student body receives online communication that is considered to be particularly disturbing or breaks the law.
- We immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation.

4. Managing the IT infrastructure

4.1. Internet access, security and filtering

School 21:

- Informs all users that internet, email and productivity software use can be and is monitored. This is both the case in school, when using a school device or the school's internet systems, or, for students, at home when using a school-issued mobile device (iPad).
- Has internet provided through RM broadband, which is a UK Safer Internet Centre recognised educational internet service provider.
- Uses Securly's filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming etc.). All changes to the filtering policy are consulted on, logged and only available to staff with the approved 'web filtering management' status (the IT team and the Online Safety Coordinator).
- Ensures network health through use of Microsoft's Windows 10 antivirus software.
- Uses DfE approved systems including DfE S2S to send 'protect-level' (sensitive personal) data over the internet.
- Uses encrypted cloud-based services where staff need to access 'protect-level' (sensitive personal) data off-site.
- Works in partnership with Google and Securly to ensure any concerns about the system are communicated so that systems remain robust and protect students.

4.2. Network management

School 21

- Uses individual, audited logins for all students from Year 3 to Year 13, and all adult users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and internet web sites, where useful.
- Has additional local network monitoring/auditing software installed.
- Ensures the Network Manager is up-to-date with services and policies related to network management safety.
- Has daily backup of school data (admin and curriculum).
- Uses secure, cloud storage for data storage and backup that conforms to DfE guidance.
- Storage of all data the school conforms to the EU and UK data protection requirements.
- Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, School 21:

- Ensures staff read, understand the school's Online Safety Policy. Following this, they sign the Online Acceptable Use Agreement and are set-up with internet, email access and network access.
- Access to online services is through a unique, audited username and password. The same credentials are used to access the school's network. All pupils in Year 3 and above have their own unique username and password which gives them access to the Internet and other services.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to log off when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up-to-date virus protection.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety policy is followed.
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems.
- Does not allow any outside agencies to access the network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems.
- Has a clear disaster recovery system in place that includes a secure, remote offsite backup of data.
- Uses secure data transfer. This includes DfE secure S2S website for all CTF files sent to other schools.
- Ensures that all student level data or personal data sent over the internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Has a wireless network which is secured to industry, enterprise standard security level.
- Has ensured that all IT and communications systems have been installed professionally and are regularly reviewed to ensure they meet health and safety standards.

4.3. Password policy

- School 21 makes it clear that staff and pupils must always keep their passwords private - they must not share with others.
- If a password is compromised the IT Manager and Online Safety Coordinator should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- A password policy has been applied to the network which forces all users to set a secure password and change regularly (Usually 60 days).
- For mobile devices, a secure pin is required to unlock the device at all times.
- Staff who have access and use critical or sensitive systems are strongly advised to use two factor authentication to further enhance security.

4.4. Email

School 21:

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Uses anonymous or group email addresses, for example info@school21.org.uk or department email addresses.
- Will contact the Police if one of our staff or students receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Will use a number of technologies to help protect users and systems from unsolicited, spam or infected emails.

Pupils:

- Students are taught about the online safety of using email both in school and at home.

Staff:

- Staff only use the school email system for professional purposes.
- Never use email to transfer staff or student personal data. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.
- Should never put personal or identifiable information (such as a pupil’s name) in the subject line of an email.
- The language in which email is written is often less formal and more open to misinterpretation than a written memo or a formal letter. Remember that email should be laid out and formulated to School 21 standards for written communication.
- All school email is disclosable under the Freedom of Information and Data Protection legislation. Beware that anything you write in an email could potentially be made public.

- Emails can remain in a system or a period of time after you have deleted them. You must remember that although you may have deleted your copy of the email, the recipients may not and therefore there will still be copies in existence. These copies could be discloseable under the Freedom of Information Act 2000 and the Data Protection Act 1998.
- Agreement entered into an email can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.
- Email is primarily a communication tool, and email applications are not designed for keeping email as a record. Email that needs to be kept should be identified by content e.g. does it form part of a pupil record? The retention of the email can then correspond with the classes of record according to content in the Records Management Policy. All attachments in email should be saved into an appropriate electronic filing system or printed out and placed in paper files.

4.5. School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- The school website complies with statutory DfE requirements.
- The contact details on the website will be the school's address, email and telephone number. Staff or students' personal information will not be published, unless consent has been given.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- Student photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- The administrator account for the school website will be safeguarded with an appropriately strong password.

4.6. Online learning spaces

- All members of staff manage the school's online learning space (e.g. Google Classroom). Depending on their role, they have responsibility for different parts.
- All members of the school community are able to upload and share on these learning spaces.
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community.
- In school, students are only able to upload and publish within school approved cloud systems.
- Staff adhere to the safeguarding protocol for virtual learning laid out in Appendix 4

4.7. Social networking

4.7.1. Staff, volunteers and contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to the conditions set out below.

School staff will ensure that in private use:

- Any references made on social media to students, parents/carers, staff or anything related to school must be professional.
- When references to students are made, permission must be sought and names omitted.
- School staff should not be online friends with any student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.7.2. Students

- We follow guidance from the UK Safer Internet Centre to teach students about social networking, acceptable behaviours and how to report misuse, intimidation or abuse. This is delivered through our online safety curriculum work.
- Students are required to sign and follow our (age appropriate) Student Acceptable Use Agreement.

4.7.3. Parents/carers

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

4.8. CCTV and video recordings

4.8.1. CCTV operation

- We have CCTV installed (both internally and externally) in the school for the purpose of enhancing the security of the building and for staff and student safety.
- The CCTV surveillance at the school is intended for the purpose of:
    - Protecting the school buildings and school assets, both during and after school hours;
    - Promoting the health and safety of staff, students and visitors;
    - Preventing bullying
    - Reducing the incidence of crime and anti-social behaviour (including theft, vandalism);
    - Supporting the police and other government agencies with enquiries
    - Assisting in identifying, apprehending and prosecuting offenders; and
    - Ensuring that the school rules and behavioural structures are respected so that the school can be properly managed.
- The use of CCTV is clearly signposted in the school. The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.
- Some of the cameras in operation have the ability to record sound for identifications reasons.
- The operation and recordings are managed by the department heads of the facilities and IT teams, and can be requested and viewed by any member of staff. A log of all requested recordings is kept by the facilities and IT department heads. All staff are made aware of the restrictions in relation to access and disclosure of recorded images. We will not reveal any recordings or create any copies without appropriate permission.
- Recorded data is kept and stored on the school site. Recorded data will not be retained for longer than 14 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

4.8.2. Covert monitoring

The school retains the right in exceptional circumstances to set up covert monitoring. For example:

- Where there is good cause to suspect that an illegal or serious unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances, authorisation must be obtained beforehand from the Head Teacher. Covert Monitoring may take place in classrooms when the above circumstances are satisfied. Covert Monitoring used in classrooms will never be used to observe or assess a teacher's professional performance, or to contribute to capability proceedings. Covert Monitoring will cease following completion of an investigation. Cameras sited for the purpose

of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets/changing areas.

4.8.3. Data protection

- Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has the right to request access to those images.
- Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation and the GDPR.
- All requests should be made in writing to the Head Teacher or Data Protection Officer.
- Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

If the footage contains images of other individuals then the school must consider whether:

- The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals.
- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained,
- If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

The school reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

- The School will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation and the GDPR.
- CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

4.8.4. Lesson recording equipment

- We use specialist lesson recording equipment (IRIS Connect) on occasions as a tool to share best teaching practice.
- We seek permissions from parents yearly, and only record students where permission has been granted.

4.9. Data security - Management Information System access and data transfer

4.9.1. Strategic and operational practices

At this school:

- Judicium is the Senior Information Risk Officer (SIRO).
- Staff are clear who the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information asset owners on the School 21 Source.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

4.9.2. Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to logout of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time.
- All servers are in secure remote locations, and managed by Capita.

4.10. Asset disposal

- Details of all school-owned hardware are recorded in a hardware inventory.
- Details of all school-owned software are recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic
- Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

4.11. Equipment and digital content

4.11.1. Mobile devices

- Mobile devices brought into school are entirely at the staff member, student, parent or visitor's own risk.
- Mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. 'Mobile-free' signs to this effect are displayed.
- School provided or approved mobile devices will only be used as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.

- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- The school reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobile devices may be searched at any time as part of routine monitoring by request of the Headteacher.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they should schedule this outside of their student contact time.

4.11.2. Communication devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Where contact with students and their families need to occur outside of school hours and from a personal mobile phone, staff are expected to install the application “Communicator GO 5” and use it to contact families.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- In an emergency where a staff member doesn’t have access to a school-owned device, they should use their own device and hide their own mobile number (by inputting 141) for confidentiality purposes and then report the incident to the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate

examining body. This may result in the student's withdrawal from either that examination or all examinations.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- School 21 strongly advises that student mobile phones and devices should not be brought into school.
- School 21 accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school. Mobile devices will be released to parents or carers in accordance with the school policy.

4.11.3. Access, storage and syncing of school-owned devices

- For student devices, software, apps and file use are managed by the IT team.
- For staff devices, software, apps and file use are managed by the IT team unless permission has been sought and granted meaning otherwise.
- Network email and pin passwords can be reset by the IT team if access to the device is required.
- If personal accounts are used for access to a school owned mobile device, staff and students must be aware that school use will be synced to their personal cloud, and personal use may become visible in school and in the classroom.
- When a staff or student member leaves and the device is returned the staff member must remove their personal account so that the device can be factory reset and cleared for reuse.

4.11.4. Digital images and video

At School 21:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when they join and annually thereafter.
- We do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials/DVDs.
- Staff sign the school's Online Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students.
- If specific student photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.
- The school blocks and filters access to social networking sites unless there is a specific approved educational purpose.
- Students are taught about how images can be manipulated and to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their online safety scheme of work.

- Students are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.
- We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Appendix 1

Online acceptable use policy: for students

Appendix 2

Online acceptable use policy: for school staff

Appendix 3
Online acceptable use policy: for visitors

Appendix 4
Parental Acceptable Use Agreement including photo/video permission

Appendix 5
Safeguarding protocol for virtual learning

RATIONALE

In the event of school closure where virtual learning will be used to continue education. School 21 must continue to safeguard students remotely in line with guidance for the Department for Education and the Local Authority.

ROLE OF THE LOCAL AUTHORITY

The Local Authority will work with the DfE and local schools to ensure that children of critical workers and vulnerable children can attend a school or college. Local authorities have the key day-to-day responsibility for delivery of children's social care. Social workers and VSHs will continue to work with vulnerable children in this difficult period and should support these children to access this provision. There is an expectation that children with a social worker will attend provision, unless in consultation with the child's social worker and family it is agreed this is not in the best interests of the child.

KEEPING CHILDREN SAFE IN EDUCATION

KCSIE remains essential guidance for schools to follow to continue safeguarding all young people. Whilst safeguarding practices are far from business as usual the following principles remain the same:

- with regard to safeguarding, the best interests of children must always continue to come first
- if anyone in a school or college has a safeguarding concern about any child they should continue to act and act immediately a DSL or deputy should be available
- it is essential that unsuitable people are not allowed to enter the children's workforce and/or gain access to children
- children should continue to be protected when they are online

DESIGNATED SAFEGUARDING LEADS

The role and responsibilities of the Designated Safeguarding Lead remains the same in line with this policy and the Safeguarding policy.

ONLINE SAFETY IN SCHOOLS AND COLLEGES

IT Systems staff will:

- ensure all students have access to a working device
- ensure that filters and restrictions on all devices function
- ensure that any breaches of the Acceptable User Policy are reported to the relevant Head of School or DSL (where appropriate)
- maintain software to ensure that access to learning is not disrupted

Teachers will:

- Adhere to the expectations of the Acceptable User Policy
- Deliver online lessons from a living room or kitchen area (not a bedroom)
- Dress appropriately to deliver online lessons
- Copy the relevant HoY/HoS/DSL into prolonged correspondence with an individual student
- Deliver online lessons to groups of students, never one to one
- Record online lessons (only when asked to do so)
- Take an attendance register and escalate absence to the relevant HoY/HoS
- Use only their school email to contact students

Students will:

- adhere to the expectations of the Acceptable User Policy
- use only their school email to contact staff
- not invite students outside of School 21 to Google Hangout lessons
- dress appropriately to attend online lessons

Parents will:

- ensure that their child accesses online learning from a supervised location in the home.
- ensure that their child attends virtual lessons where necessary
- ensure that they put appropriate parental controls on school devices
- seek support from reputable sources to keep their children safe online

Parents can find support from the following services:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and carers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers