



ONLINE SAFETY POLICY

This policy was last reviewed by the Governing Body on the 6th June 2018.

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.

This policy is a model template that has been provided by School Improvement Liverpool in conjunction with Liverpool Safeguarding Children's Board and was adapted from and with approval from Trust net/London Grid for Learning, Online Safety Policy.

“Nothing is more important than promoting the welfare of children and protecting them from harm”

DFE, May 2016

(from the government's response to Alan Wood's, CBE – Review of the role and functions of Local Safeguarding Children Boards)

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation, sexual predation – technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.

DFE, May 2016

(from Annex C: Online Safety – Keeping Children Safe in Education)

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

TRUST net

paul.bradshaw@si.liverpool.gov.uk 01.09.16

Contents

1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring
- Data Protection

2. Education and Curriculum

- Pupil online safety curriculum
- Staff and Governor training
- Parent awareness and training

3. Expected Conduct and Incident Management

4. Managing the IT Infrastructure

- Internet access, security (virus protection) and appropriate **filtering**
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices

A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreements (Pupils – adapted for phase)

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

A3: Acceptable Use Agreement including photo/video permission (Parents)

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Clifford Holroyde SEN College 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
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

Conduct

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

Scope

This policy applies to all members of Clifford Holroyde SEN Community including ALL staff, pupils/students, volunteers, parents/carers, visitors, community users who have access to and are users of Clifford Holroyde's IT systems, both in and out of Clifford Holroyde SEN College.

Roles and responsibilities

Role	Key Responsibilities
Headteacher: Mrs J Pepa	<ul style="list-style-type: none">• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.• To take overall responsibility for online safety provision.• To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling and is compliant with the eight principles of the Data Protection Act 1998.• To ensure the school uses appropriate IT systems and services including, a filtered Internet Service.• To be responsible for ensuring that <u>ALL</u> 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' are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Role	Key Responsibilities
	<ul style="list-style-type: none"> • To receive regular monitoring reports from the Online Safety Lead. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety. • To ensure school that the school website includes relevant information and is compliant with the statutory requirements.
<p>Online Safety Lead/Designated Safeguarding Lead: Mrs K Garrett</p>	<ul style="list-style-type: none"> • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents. • Promote an awareness and commitment to online safety throughout the school community. • Ensure that online safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and appropriate filtering/monitoring issues and change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for <u>ALL</u> staff. • Oversee any pupil surveys/pupil feedback on online safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
<p>Governors including the Safeguarding Governor (including online safety): Mrs Sheila Bennett</p>	<ul style="list-style-type: none"> • To ensure that the school has in place policies and practices to keep the children and <u>ALL</u> staff safe online. • To approve the Online Safety Policy and review the effectiveness of the policy.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

Role	Key Responsibilities
	<ul style="list-style-type: none"> • To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities. • The role of the Online Safety Governor will include: regular review with the Online Safety Lead
<p>Computing Curriculum Lead: Mr W Tagoe</p>	<ul style="list-style-type: none"> • To oversee the delivery of the online safety elements of the Computing Curriculum.
<p>Network Manager/IT technician: Mr D Murphy</p>	<ul style="list-style-type: none"> • To report all online safety related issues that come to their attention, to the Online Safety Lead. • To manage the school's computer systems, ensuring <ul style="list-style-type: none"> - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus/malware/ransomware protection up to date). - access controls/encryption exist to protect personal and sensitive information held on school-owned devices. - the school's policy on appropriate web filtering and monitoring is applied and updated on a regular basis. • To 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 required. • To ensure school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Lead/DSL/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.
<p>Data and Information Managers</p>	<ul style="list-style-type: none"> • 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, stored, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

Role	Key Responsibilities
Teachers	<ul style="list-style-type: none"> • To embed online safety in the curriculum. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff, volunteers and contractors.	<ul style="list-style-type: none"> • To read, understand, sign and adhere to the school staff Acceptable Use Policy, and understand any updates - annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problems to the Online Safety Lead. • To maintain an awareness of current online safety issues and guidance e.g. through relevant CPD. • To always model safe, responsible, respectful and professional behaviours in their own use of technology. <p>Exit strategy</p> <ul style="list-style-type: none"> • At the end of the period of employment returning any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	<ul style="list-style-type: none"> • Read, understand, sign and adhere to the Pupil /Student Acceptable Use Agreement, annually. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To understand the importance of adopting safe, responsible and respectful behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school. • To contribute to any 'pupil voice'/surveys that gathers information of their online experiences.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

Role	Key Responsibilities
Parents/carers	<ul style="list-style-type: none"> • To read, understand and promote the school's Pupil Acceptable Use Agreement with their child. • 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, including social media and the school's use of photographic and video images
External groups including Parent groups	<ul style="list-style-type: none"> • Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within school. • To support the school in promoting online safety. • To model safe, responsible, respectful and positive behaviours in their own use of technology.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Communication:

The policy will be communicated to staff/pupils/community and ICT service providers in the following ways:

- Policy to be posted on the school website, staffroom, Staff share system and ICT room.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable Use Agreements discussed with staff and pupils at the start of each year. Acceptable Use Agreements to be issued to whole school community, on entry to the school.

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 Lead to act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Lead 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 complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The Online Safety Policy is referenced within other school policies (e.g. Safeguarding and Child Protection Policy, Anti-Bullying Policy, PSHE, Computing Curriculum Policy).

- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety Policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the ICT Curriculum/PSHE curriculum and other curriculum areas as they are relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the Pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe, responsible, respectful and professional 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.

Staff and Governor training

This school:

- 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 [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Policies/Agreements.

Parent awareness and training

This school:

- Provides induction for parents which includes online safety information through the admission process.
- Runs a programme of online safety advice, guidance and training for parents through the school's parent's afternoons as well as providing online safety advice via the schools' website and facebook page. It should be noted that one to one guidance will also be given to parents as and when required.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

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

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;

Parents/Carers

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

Incident Management

In this school:

- 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. School Improvement Liverpool, UK Safer Internet Centre Helpline (0844 3814772/helpline@saferinternet.org.uk), CEOP, Prevent Officer, Merseyside Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of any online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Merseyside Police, Internet Watch Foundation and inform the Local Authority.

4. Managing IT and Communication System

Internet access, security (virus protection) and appropriate filtering and monitoring

This school:

- informs all users that Internet/email use is monitored;
- has filtered, secure broadband connectivity provided by the school's ICT service provider Apex Computing Services Ltd who provide a safe and secure 10Mbps broadband connection.
- uses a cloud-based filtering system called Surf Protect by Exa Network which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses user level filtering; Clifford Holroyde is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible. With this in mind the E-Safe system has been installed onto the School's Server.
- ensures network health through use of ESET anti-virus software;

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

- Uses approved systems to send 'protect-level' (sensitive personal) data over the Internet.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

Network management (user access, backup)

This school

- Uses individual, audited log-ins for all 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; Ranger is installed and used by staff for this
- Ensures the Systems Administrator/Network Manager is up-to-date with their technical knowledge;
- Has daily off-site back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform 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, Clifford Holroyde:

Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password.

- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use 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/malware/ransomware protection;

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

- Makes clear that staff are responsible for ensuring that any computer/laptop/mobile device loaned to them by the school, is used only to support their professional responsibilities.
- Makes clear that staff accessing Local Authority systems do so in accordance with any corporate Liverpool City Council Policies;
- Maintains equipment to ensure Health and Safety 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 approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off-site back up of data;
- This school uses secure data transfer.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted.
- Our wireless network has been secured to industry standard Enterprise security level / appropriate standards suitable educational use;
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

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

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

- We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use school e-mail systems on the school system.
- Staff will use the school e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil 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.

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 web site complies with statutory DFE requirements;
- 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;
- 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.

Social Networking

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 pupils 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.
- For the use of any school approved social networking will adhere to school's Communications Policy.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- Never post images or videos of pupils/students.
- School staff should not be online friends with any pupils/students or parents/carers of pupils/students.
- If they receive a friend request from a pupil/student or parent/carer they should decline the invite and inform their Line Manager.
- 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 and privacy settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, safe, responsible, respectful and acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- 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.
- Are encouraged to model safe, responsible and respectful use of social media for their children to emulate.
- As a school we believe that parents should be discouraged from using social media to criticise teaching staff and to make comments about our school and the community it serves. If you feel that you have any issues regarding your child's schooling, please make an appointment to come and talk to us. We are always happy to listen.

CCTV

- We have CCTV in the school as part of our surveillance for staff and pupil safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

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

Technical Solutions

- Staff have secure areas on the network to store sensitive files
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- All servers are in secure, lockable locations and managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory, including hardware on loan to named staff members.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

6. Equipment and Digital Content

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

- Mobile devices brought into school are entirely at the staff member, pupils/students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No pupil should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- If pupils bring mobile devices into school they are expected to hand in at reception and placed within a pupils personal wallet and in the safe, they will be handed back at the end of the school 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.
- Staff mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- 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 mobiles devices may be searched at any time as part of routine monitoring.
- If a pupil 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 may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Storage, Synchronizing and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the Pupil's withdrawal from either that examination or all examinations.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Pupils will be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such mobile devices will be set up so that only those features required for the activity will be enabled.

Staff use of personal devices

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- 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.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- 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 (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school admission process. This is in effect for the length of time the pupil remains on roll or until parent's /carers state they no longer give consent.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, 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/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work
- Pupils 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.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

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.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Appendix 1

	Name of School	Clifford Holroyde SEN College
	AUP review Date	6th June 2018
	Date of next Review	6th June 2019
	Who reviewed this AUP?	Governing Body

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. email, Internet, intranet, network resources, learning platform, software, communication tools, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems, *or any Local Authority (LA) system I have access to.*
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
This is currently: Office 365
- I will only use the approved Office 365, with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / school named contact*.
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
 - I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will follow the school's policy on use of mobile phones / devices at school and *will not take into classrooms and only use in staff areas*
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access school resources remotely (such as from home) using the *school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert Clifford Holroyde's child protection officer / appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Headteacher / Designated Safeguarding Lead.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Headteacher / Safeguarding Lead on their request.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16

- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any LA system I have access to in accordance with their policies.
- **Staff that have a teaching role only:** I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand th

e school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature Date.....

Full Name (printed)

Job title / Role

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature Date.....

Full Name (printed)

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



Appendix 2

Clifford Holroyde SEN College Pupil Acceptable Use Agreement

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's computers for appropriate school activities and learning and am aware that the school can monitor my internet use.
2. I will not bring files into school that can harm the school network or be used to circumvent school security tools
3. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will use the Internet responsibly and will not visit web sites that are inappropriate for the school or my key stage.
6. I will only e-mail or contact people I know, or those approved as part of learning activities
7. The messages I send, or information I upload, will always be polite and sensible. All messages I send reflect on me and the school.
8. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file.
9. I will not give my personal information that could be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
11. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.
12. I am aware that some websites, games and social networks have age restrictions and I should respect this.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

TRUST net

paul.bradshaw@si.liverpool.gov.uk 01.09.16

13. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.

I have read and understand these rules and agree to them.

Signed:

Date:

Appendix 3



Clifford Holroyde Parent Acceptable Use Policy

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my Son / Ward access to:

- the Internet at school
- the school's chosen email system
- the school's online managed learning environment
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. ✓

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me. ✓

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this. ✓

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities. ✓

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose. ✓

I will not take and then share online, photographs of other children (or staff) at school events without permission. ✓

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Social networking and media sites: I understand that the school has a clear policy on “The use of social networking and media sites” and I support this.



I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.



I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.



My Son / Ward Name: _____

Parent / guardian signature: _____

Date: ___/___/___



Clifford Holroyde School use of digital Images and video



To comply with the Data Protection Act 1998, we need your permission before we can photograph or make recordings of your daughter / son.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.

If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Staffs are not allowed to take photographs or videos on their personal equipment.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity;
e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.
- Your child's image being used for presentation purposes around the school;
e.g. in class or wider school wall displays or PowerPoint© presentations.
- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators;
e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.

(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:

<https://www.thinkuknow.co.uk/parents/browser-safety/>

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

TRUST net

paul.bradshaw@si.liverpool.gov.uk 01.09.16

This Policy was last reviewed by the governing body on 6th June 2018

Signed
Chair Of Governors

Next review date: June 2018

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro