Policy Title:	Using Technology Safely
Function:	This policy sets out guidance for staff, students, parents and governors, and other members of our school community, and forms part of the School's statutory Safeguarding Policy.
Status:	Non-statutory, but part of Safeguarding policy
Audience:	All staff, students, parents, governors
Ownership / Implementation:	The Principal has overall responsibility for ensuring that this policy is implemented.
Implementation Date:	April 2016
Review period:	Annually
Last Reviewed:	April 2016

Using Technology Safely Policy

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.

Table of Contents

1. Introduction and overview

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Compass School Southwark 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	Contact	Coduct
• Exposure to inappropriate content • Lifestyle websites promoting harmful behaviour • Hate content	• Grooming (Child Sexual Exploitation, radicalisation, etc) • Online bullying in all forms • Social and commercial identity theft	• Aggressive behaviours (including bullying) • Privacy, including disclosure of personal information • Digital footprint and online reputation • Health and well-being • Sexting • Copyright

This policy applies to all members of Compass School Southwark (staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Compass School IT systems and devices, both in and out of Compass School Southwark.

Roles and responsibilities

Role	Key Responsibilities
Principal	• Must be adequately trained in off-line 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 (SIRO) ensuring school's provision follows best practice in information handling • To ensure the school uses appropriate IT systems and services • 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 Students, including risk of children being radicalised • 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 school website includes relevant information
Designated Child Protection Lead	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • To communicate regularly with SLT and the child protection and safeguarding governor to discuss current issues, review incident logs and filtering/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 all staff • Oversee any Student surveys / Student feedback on online safety issues • Liaise with the Local Authority and other relevant agencies

Role	Key Responsibilities
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns
Child protection and safeguarding governor	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Using Technology Safely 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 • The role of the online safety Governor will include: regular review with the designated Child Protection lead
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum
Network Manager/technician	• To report online safety related issues that come to their attention, to the designated Child Protection lead • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's Using Technology Safely policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the designated child protection lead/Principal • To ensure appropriate backup procedures/ disaster recovery plans 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. • The school must be registered with Information Commissioner
Teachers	• To embed online safety in the curriculum • To supervise and guide Students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)

Role	Key Responsibilities
	• To ensure that Students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates termly. The AUP is signed by new staff on induction • To report any suspected misuse or problem to the designated child protection lead • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset
Students	• Read, understand, sign and adhere to the Student Acceptable Use Policy termly • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'student voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the school's Student 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 Students' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology

Communication

This policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the school website and staff room
- Termly review and agreement as part of login procedure for staff and students
- Policy to be part of the school induction pack for new staff
- Regular updates and training on online safety for all staff
- Acceptable Use Agreements discussed with staff and students at the start of each year
- Acceptable Use Agreements to be issued to all members of the school community at the start of each academy year, or on entry to the school

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and students are given information about infringements in use and possible sanctions
- The Designated Child Protection lead acts as the first point of contact for any incident
- Any suspected online risk or infringement is reported on the same day
- Any concern about staff misuse is always referred directly to the Principal unless the concern is about the Principal, in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority Designated Officer)

Review and Monitoring

The Using Technology Safely Policy is referenced with other school policies, and is reviewed annually, or when any significant changes occur with regard to the technologies in use within the school.

All amendments to the policy are disseminated to all members of staff and all students.

2. Education and Curriculum

Compass School Southwark has a clear and progressive online safety education programme which is accessible to all members of our community.

For students this school:

- has a clear, progressive online safety education programme as part of the Computing and Relating curriculums as appropriate. 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 students about their responsibilities through the Student Acceptable Use Agreement(s);
- 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 Students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure students only use school-approved systems and publish within appropriately secure / age-appropriate environments.

For staff and governors 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 Agreements.

For parents and carers this school:

- provides induction for parents which includes online safety;
- provides annual e-safety letter with tips and contacts (during Safer Internet Week)

3. Expected Conduct and Incident Management

Expected conduct

In this school, all users:

- are responsible for using the technology in school in accordance with the relevant AUPs;
- understand the significance, and consequences, of misuse/access to inappropriate material;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting online safety practice both in and out of school;
- know and understand policies on the use of mobile/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 where students have more flexible access;
- know to take professional, reasonable precautions when working with students, previewing websites before use and ensuring that students use age-appropriate sites.

Parents/Carers

- should provide consent for students 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 are dealt with quickly and sensitively, through escalation processes;
- support is actively sought from other agencies as needed (i.e. LA, UK Safer Internet Centre helpline, CEOP, PREVENT Officer, Police) 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 online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or students 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 – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication Systems

Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- uses the Lightspeed filtering system which blocks sites falling into inappropriate categories;
- Uses DfE and LA approved systems to send sensitive personal data over the Internet;
- Uses encrypted devices or secure remote access where staff need to access 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 Impero 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- 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, this school:

- Ensures staff read and sign that they have understood the school's Using Technology Safely policy. Following this, they are set-up with Internet, email access and network access.
- All students 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 students should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for students and one for staff. Staff and students 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;
- 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; 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;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

This school makes it clear that staff and students must always keep their passwords private, and must not share this 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, and passwords are changed regularly.

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;
- We use anonymous or group e-mail addresses, for example info@compass-schools.com /recruitment@compass-schools.com;
- Will contact the Police if one of our staff or students 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;

Students:

- Are taught about the online safety and 'netiquette' of using e-mail both in school and at home;

Staff:

- Will use school e-mail systems for professional purposes only;
- Access in school to external personal e-mail accounts may be blocked;
- 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.

School website

- The Principal, 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 Students' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

School staff and volunteers will ensure that:

- Professional and private communication are separate;
- No reference should be made in social media to students, parents/carers or school staff;
- School staff should not be online friends with any student of the school, without exception;
- 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.

Students:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work;
- Students are required to sign and follow our Acceptable Use Policy.

Parents/carers:

- Parents are reminded about social networking risks and protocols through our student AUP 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.

5. Equipment and Digital Content

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

- The School strongly advises that student mobile phones and devices should not be 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;
- Staff, volunteers and visitors must only use personal mobile phones in designated staff areas or personal office areas. Mobile phones should remain on silent during the school day;
- Student personal mobile devices brought into school must be turned off and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy;
- Personal mobile devices will not be used during lessons unless permission has been given by the classroom teacher for a specific activity;
- 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;
- 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;
- No images or videos should be taken on any 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 Principal. 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;
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities;
- 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;
- 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 Principal / 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 agreement form when their daughter/son joins the school (or annually).;
- 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 Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of students;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Students 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;
- 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 A - Acceptable use agreement – STUDENT

Using Technology Safely

Acceptable use agreement – STUDENT

Students are expected to uphold the Compass School values of 'aspiration', 'integrity', 'exploration' and 'resilience' at all times, even online. This agreement includes use of your own devices as well as school devices.

1. I will only use the school's computers for school work, homework, exploration projects and as directed.
2. I will not bring files into school (on removable devices or online file storage) without permission.
3. I will not upload or download any inappropriate material to my workspace on the network.
4. I will only edit or delete my own files and not view, or change, other people's files without their permission.
5. I will keep my login details, and passwords, secret from other students.
6. I will use the Internet responsibly and will not visit website I know are banned by the school.
7. During lessons, I will only visit websites that are appropriate for my studies.
8. I will only email people that I know, or those who are approved by my teachers.
9. The messages that I send, or information I upload, will always be polite, sensible and demonstrating integrity.
10. I will not open attachments, or download files, unless I have permission or I know and trust the person that has sent them.
11. I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
12. 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.
13. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will save it and talk to a teacher or confide using the Confide button.
14. I am aware that some websites and social networks have age restrictions and I should respect this.
15. 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.

Appendix B - Acceptable use agreement – STAFF, VOLUNTEERS, GOVERNORS

Using Technology Safely

Acceptable use agreement – STAFF, VOLUNTEERS, GOVERNORS

Staff, volunteers and governors are expected to uphold the Compass School values of 'aspiration', 'integrity', 'exploration' and 'resilience' at all times, even online. This agreement applies to all digital technologies used in school, and any school devices used outside of school.

1. I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Principal and Governing Body.
2. I will not disclose my password(s) for any devices or websites associated with the school.
3. 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.
4. I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.
5. 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.
6. I will not engage in any online activity that may compromise my professional responsibilities or bring the school into disrepute.
7. I will only use the approved Microsoft Exchange email system for any school business.
8. I will only use the approved Microsoft Exchange Email system or the Management Information System (Arbor) to communicate with Students or parents/carers, and only communicate with them on appropriate school business.
9. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
10. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the Director of Business and Operations in the first instance.
11. 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.
12. 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.
13. I 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 and secure.

15. I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of Students or staff and will not store any such images or videos at home.
16. I will follow the school's policy on use of mobile phones / devices at school and will not take these devices into classrooms (personal mobile phones should only be used in the staff room or own private offices).
17. 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 shared drive (Staff Shared > Community > Photos).
18. I will use the school's Learning Platform (My Learning) in accordance with school protocols.
19. 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.
20. I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
21. 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.
22. I will only access school resources remotely (such as from home) using the Microsoft Remote Desktop application and follow e-security protocols to interact with them.
23. 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.
24. I understand that data protection policy requires that any information seen by me with regard to staff or Student 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.
25. I will alert the designated child protection officer if I feel the behaviour of any child may be a cause for concern.
26. I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or Students, which I believe may be inappropriate or concerning in any way, to the designated Child Protection lead.
27. I understand that all Internet and network traffic / usage is logged and this information is available to the Principal and Safeguarding lead on request.
28. I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
29. I will embed the school's on-line safety / digital literacy / counter extremism curriculum into my teaching and/or other interactions with students.