VOYAGE LEARNING CAMPUS

ONLINE SAFETY POLICY

This policy has been adopted by SLT on:	
Date adopted:	12th June 2018
Signed:	
Next review due:	June 2019

Voyage Learning Campus (VLC)
Online Safety Policy

Policy to be read in conjunction with the following document:

- ***VLC Safeguarding Policy***
- ***VLC Cyberbullying Policy***
- ***VLC Use of digital and video images Policy***
- ***VLC Electronic Devices – Searching and Deletion Policy***
- ***VLC Virtual Learning Environment (VLE) Policy***
- ***DfE Guidance – Searching, screening and confiscation advice (February 2014)***
- ***DfE Guidance – Keeping children safe in education***
- ***VLC Portable Equipment Loan Policy***
- ***VLC Data Protection Policy***
- ***VLC Data Security Plan***

Contents

Appendices:

1. Acceptable Use Policy for staff – Staff agreement form
2. Acceptable Use Agreement forms for KS1, KS2 and KS3
3. Record of Online Safety Incident sheet

1. Introduction and Overview

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the Campus community at the VLC with respect to the use of ICT-based technologies.
- Safeguard and protect the students and staff of the VLC.
- Assist staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to the responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyber bullying.
- Ensure that all members of the Campus 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 the VLC can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites; radicalisation and extremism
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation

- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film) (Ref Ofsted 2013)

Scope of the policy (from South West Grid for Learning)

This policy applies to all members of the VLC community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of Campus ICT systems, both in and out of the VLC.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the Campus site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the Campus, but is linked to membership of the Campus. The 2011 Education Act ***(amended November 2013)*** increased these powers with regard to the searching for and of electronic devices and the deletion of data ***(see appendix 8 for template policy).*** In the case of both acts, action can only be taken over issues covered by the published Behaviour for Learning Policy.

The VLC will deal with such incidents within this policy and associated behaviour and anti-bullying and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place away from the Campus.

1.2 Roles and Responsibilities

Role	Key Responsibilities
Principal	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security (SIRO – Senior Information Risk Owner - https://www.gov.uk/service-manual/technology/securing-your-information) • To ensure the Campus uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. SWGfL • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious Online Safety incident. • To receive regular monitoring reports from the Online Safety Co-ordinator • To ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures

Role	Key Responsibilities

Online Safety Co-ordinator and Designated Safeguarding Lead	• takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the Campus Online Safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the VLC
	• ensures that Online Safety education is embedded across the curriculum
	• communicate regularly with SLT and the designated Online Safety Management Committee member to discuss current issues, review incident logs and filtering / change control logs
	• ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident
	• ensure that an Online Safety incident log is kept up to date
	• facilitate training and advice for all staff
	• 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 issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media
	• To oversee the delivery of the Online Safety element of the computing curriculum
	• To liaise with the Online Learning & Network Manager regularly

Named Management Committee member	• To ensure that the Campus follows all current Online Safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Management Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Management Committee has taken on the role of Online Safety member • To support the Campus in encouraging parents / carers and the wider community to become engaged in Online Safety activities • The role of the Online Safety Management Committee member will include: • regular review with the Online Safety Co-ordinator including Online Safety incident logs, filtering / change control logs.

Role	Key Responsibilities
Online Learning & Network Manager	• To report any online safety related issues that arises, to the Online Safety Co-ordinator. • To ensure that users may only access the VLC's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the VLC's IT network. • To ensure that access controls / encryption exist to protect personal and sensitive information held on Campus-owned devices. • To ensure the VLC's policy on web filtering is applied and updated on a regular basis. • SWGfL is informed of issues relating to the filtering applied by the Grid. • To ensure that all data held on students on the Virtual Learning Environment is adequately protected. • Keeps up to date with the VLC'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 • To ensure that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Co-ordinator and Principal for investigation. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the VLC's e-security and technical procedures. • To ensure that all data held on students on the VLC office machines have appropriate access controls in place.
SWGfL Nominated contact(s)	• To ensure all SWGfL services are managed on behalf of the Campus including maintaining the SWGfL database of access accounts.
Teachers	• To embed Online Safety issues in all aspects of the curriculum and other Campus activities. • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Campus activities if relevant). • 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.

Role	Key Responsibilities
All staff	• To read, understand and help promote the Campus's Online Safety policies and guidance. • To read, understand, sign and adhere to the Campus Staff Acceptable Use Policy. • To be aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Campus policies with regard to these devices. • To report any suspected misuse or problem to the Online Safety Co-ordinator and record misuse in the incidents log. • 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. • To ensure that any digital communications with students should be on a professional level and only through Campus based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Students	• Read, understand, sign and adhere to the Acceptable Use Policy (note: at KS1 it would be expected that parents / carers would sign on behalf of the students). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • 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 know and understand Campus policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand Campus policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good Online Safety practice when using digital technologies out of Campus and realise that the VLC's Online Safety Policy covers their actions out of Campus, if related to their membership of the Campus. • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in Campus and at home • To help the Campus in the creation/ review of Online Safety policies.
Campus Student & Family Liaison Officer	• Educating parents and raising awareness as instructed by the Principal.

Role	Key Responsibilities
Parents / carers	• To support the Campus in promoting Online Safety and endorse the Students' Acceptable Use Policy which includes the students' use of the internet and the Campus's use of photographic and video images. • To read, understand and promote the Campus Student Acceptable Use Policy with their children. • To access the Campus website / student records in accordance with the relevant Campus Acceptable Use Agreement. • To consult with the Campus if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within Campus

1.3 Communication:

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

- Policy to be posted on the VLC website
- Policy to be part of VLC induction pack for new staff
- Acceptable use agreements forms discussed with students and signed when they start at VLC.
- Acceptable use agreements forms to be issued to VLC staff and signed, and reviewed on a yearly basis
- Student's acceptable use agreement forms to be held in personal files

1.4 Handling complaints:

- The VLC will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a VLC computer or mobile device. Neither the VLC nor the Local Authority (LA) can accept liability for material accessed, or any consequences of Internet access.

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

    - interview/counselling by Heads of Centres / Online Safety Co-ordinator / Principal;
    - informing parents / carers;
    - removal of Internet, computer access, or other ICT services for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
    - Referral to LA / Police.

- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal.

- Complaints of cyber bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with VLC / LA child protection procedures.

1.5 Review and Monitoring

The Online Safety policy is referenced from within other VLC policies: Safeguarding policy, Anti-Bullying & Harassment policy and in the VLC Development Plan and Behaviour for Learning policy.

- The VLC has an Online Safety Co-ordinator who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the Campus
- The Online Safety policy has been written by the VLC Online Safety Coordinator and reviewed by all staff outlined in 1.2 to ensure it is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team.

2. Education and Curriculum

2.1 Student Online Safety curriculum

The VLC

- Has a clear, progressive Online Safety education programme as part of the computing curriculum / PSHE curriculum. It is built on LA / SWGfL e-Safeguarding and e-literacy framework for EYFS to Y11 national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

    - to STOP and THINK before they CLICK;
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older students] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;

- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older students] to understand why and how some people will 'groom' young people for sexual reasons;
- To understand the impact of cyber bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
- To understand the impact of extremism, and how to identify if they may be a target of radicalisation.

- Plans internet 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 an Acceptable Use Policy which every student will sign before they are able to use ICT equipment and services.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.

2.2 Staff and Management Committee training

The VLC:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on Online Safety issues.
- Provides, as part of the induction process, all new staff with information and guidance on the Safeguarding policy and the Campus's ICT Acceptable Use Policies.

2.3 Parent / carer awareness and training

The VLC

- Runs a rolling programme of advice, guidance and training for parents / carers, including:
    - Parents / carers will be made aware of the VLC IT Acceptable Use Agreement Form their child will need to sign, to ensure that principles of safe online behaviour are made clear;
    - Information leaflets; in VLC newsletters and on the VLC website;
    - Suggestions for safe internet use at home;
    - Provision of information about national support sites for parents.

3.1 Expected Conduct and Incident management

Expected conduct

In the VLC, all users:

- are responsible for using the VLC ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to Campus systems. (at KS1 it would be expected that parents/carers would sign on behalf of the students)
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good Online Safety practice when using digital technologies out of Campus and realise that the Campus's Online Safety Policy covers their actions out of Campus, if related to their membership of the Campus. This includes, but is not limited to, use of VLC equipment out of centre.
- will be expected to know and understand Campus policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Campus policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the VLC's Online Safety policy and using the Campus ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

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 at time of their child's entry to the VLC

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

Incident Management

In the VLC:

- There is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the VLC's escalation processes.
- Support is actively sought from other agencies as needed (e.g. the LA and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online Safety issues
- Monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in Online Safety within the VLC. The records are reviewed/audited and reported to the Campus's Senior Leadership Team, Management Committee and Local Authority
- Parents/carers are specifically informed of Online Safety incidents involving young people for whom they are responsible
- We will contact the police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

4.1 Internet access, security (virus protection) and filtering

The VLC:

- Has the educational filtered secure broadband connectivity through the SWGfL;
- Uses the SWGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status;
- Uses user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of anti-virus software (from SWGfL) etc and network set-up so staff and students cannot download executable files;
- Uses secure email to send personal data over the internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform;
- Only unblocks other external social networking sites for specific purposes;
- Blocked student access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;

- Works in partnership with the SWGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures students only publish within an appropriately secure environment : the Campus's learning environment/ SWGfL secure platforms etc.
- Requires staff to preview websites before use and encourages use of the Campus's VLE as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for internet use to match students' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search
- Never allow / is vigilant when conducting 'raw' image search with students e.g. Google image search;
- Informs all users that internet use and emails are monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly person responsible for URL filtering. Our system administrator(s) logs or escalates as appropriate to the technical service provider or SWGfL helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for students, staff and parents / carers.
- Immediately refers any material we suspect is illegal to the appropriate authorities – police – and the LA.

4.2 Network management (user access, backup)

The VLC

- Uses individual, audited log-ins for all users;
- Requires the technical support provider to be up-to-date with SWGfL services and policies;
- Storage of all data within the VLC will conform to the GDPR (May 2018) requirements
- Students and staff using mobile technology, where storage of data is online, will conform to the GDPR where storage is hosted within the EU.

To ensure the network is used safely, the VLC:

- Ensures staff read and sign that they have understood the Campus'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;

- Staff network access to the management information system is controlled through their individual password for data security purposes;
- We provide students with an individual network log-in username;
- All students have their own unique username and password which gives them access to the Internet;
- **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 as these have far less security restrictions and inappropriate use could damage files or the network;
- 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 always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the VLC provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any equipment loaned to them by the VLC, is used solely to support their professional responsibilities.
- Makes clear that students are responsible for ensuring that all equipment loaned to them by VLC is used solely for the purpose of their education and must not be used for any other reason, or by other family members.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures all equipment has been PAT tested by our compliance contractor as required by law;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Provides students and staff with access to content and resources through the SWGfL which staff and students access using their username and password;
- Makes clear responsibilities for the daily back up of the IT Network and systems;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Uses the DfE secure S2S website for all CTF files sent to other schools;

- Uses the Local Authority Anycomms system for secure transfer of confidential files, including CTF files.
- Follows ISP advice on local area and wide area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the Campus ICT systems regularly with regard to health and safety and security.

4.3 Passwords policy

- This VLC makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find.
- All staff have their own unique username and private passwords to access Campus systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.
- Staff are required to change their passwords on an annual basis, using a strong password, which must include at least one lowercase letter, one uppercase letter, one number and one special character, and must be at least 8 characters long.

4.4 E-mail

The VLC

- Provides staff and some students (KS3 & KS4) with an email account for their professional / educational use and makes clear personal email should be through a separate account;
- 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;
- Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of SWGfL-provided technologies to help protect users and systems in the Campus, including desktop anti-virus products, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Students:

- Students are introduced to emails as part of the ICT/Computing scheme of work.

- Students may be allocated a VLC email address for the purpose of receiving VLC communications and accessing VLC online learning materials.
- Students are expected to check their VLC e-mail address, when in school, on a frequent basis in order to stay current with VLC communications.
- Students may only use approved email address accounts on the VLC system
- Students must not use their VLC email address to sign-up to any website, social media network or any other online service unless authorised to do so by VLC.
- The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, radicalization / extremism, or any other use which may be likely to cause offence. Action will be taken in all cases. It is also forbidden to send large volume Emails (spamming).
- Students will not reveal their password to anyone. If you think someone has obtained your password, contact a member of ICT Support immediately.
- Students should tell a teacher immediately if they receive an offensive email.
- Students are aware that staff have access to student email accounts and all content within, for the purpose of safeguarding and monitoring email activity.
- Students are taught about the safety and 'netiquette' of using e-mail:
    - that an e-mail is a form of publishing where the message should be clear, short and concise;
    - they must not reveal private details of themselves or any other student or staff member in e-mail communication, such as address, telephone number, etc.;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - that they should think carefully before sending any attachments;
    - not to respond to malicious or threatening messages;
    - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted.
- Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities will be reported to the Principal.

Other Considerations:

- Remember that you are a representative of the school on a global public system. You may be alone with your computer, but what you say and do can be viewed by others. Never swear, be offensive or use inappropriate language. Illegal activities of any kind are strictly forbidden.

- Be brief. Few people will bother to read a long message. Proof read your message to ensure that it is error free and easy to understand.
- Remember that humour and satire are very often misinterpreted.
- Cite references for any facts that you present. Do not copy other peoples work and imply that it is your own. If you do so, you are almost certainly guilty of plagiarism. Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.
- Respect the rights and beliefs of others.
- Students sign the ICT Agreement Form to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use authorised email systems on the Campus system
- Staff only use Campus e-mail systems for professional purposes
- Access in the Campus to external personal email accounts may be blocked
- We use secure, LA / DfE approved systems to transfer staff and student personal data. These include: S2S (for Campus to School transfer); B2B and AnycommsPlus*;*
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on Campus headed paper. That it should follow the Campus 'house-style':
    - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
    - the sending of chain letters is not permitted;
    - embedding adverts is not allowed;

- All staff sign our Staff Agreement Use Form to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

4.5 The VLC website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authors: e.g. School Operations Manager, Online Learning Co-ordinator and PA to the Principal
- The VLC website complies with the statutory DfE guidelines for publications;
- Most material is the Campus'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;
- The point of contact on the web site is the VLC address, telephone number and we use a general email contact address - admin@voyagelearningcampus.org.uk. Home information or individual e-mail identities will not be published;
- Photographs of students and / or staff 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 Campus website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

4.6 Virtual Learning Environment (VLE)

- Uploading of information on the VLC's virtual learning environment is shared between different staff members according to their responsibilities;
- Photographs and videos uploaded to the Campus VLE will only be accessible by all members of the Campus community;
- In Campus, students are only able to upload and publish within Campus approved and closed systems, such as the VLE.
- Please refer to the full VLC Virtual Learning Environment (VLE) Policy.

4.7 Social networking

- 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 VLC's preferred system for such communications.

Campus staff will ensure that in private use:

- No reference should be made in social media to students / students, parents / carers or Campus staff
- They do not engage in online discussion on personal matters relating to members of the Campus community
- Personal opinions should not be attributed to the Campus or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.7 Video Conferencing

The VLC

- Uses Microsoft© Lync (Office 365) and the VLE (Canvas LMS) for video conferencing activity;
- Only uses approved or checked webcam sites.

4.8 CCTV

- 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.
- We record video conferencing and online lessons for quality and training purposes, and for use on the VLE. Where possible, student interaction will be edited out of any video used for the VLE.

4.9 Data Storage

- Only school related work, not personal files, shall be stored on the school network and the VLC OneDrive

- All users are responsible for keeping their personal storage across all VLC systems organised, up-to-date and relevant. Old / unused files should be deleted from the network in line with the VLC Retention Policy.

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

Strategic and operational practices

At the VLC:

- The Principal is the Senior Information Risk Officer (SIRO);
- We ensure staff know who to report any incidents where data protection may have been compromised;
- All staff are enhanced DBS checked and records are held in one central record with the Schools Operations Manager;
- We ensure ALL the following Campus stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - staff
    - students
    - parents / carers

  This makes clear staff responsibilities with regard to data security, passwords and access.
- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any protected and restricted material must be encrypted if the material is to be removed from the Campus and limit such data removal.
- We ensure Campus staff with access to setting-up usernames and passwords for email, network access and VLE access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which no longer needs to be stored.

5.2 Data transfer

- Staff have secure area(s) on the network to store sensitive documents or photographs
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use Microsoft OneDrive, for any member of staff has to access sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- Back up is carried out using external hard drives and kept next to servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment

where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data.

- Portable equipment loaned by the VLC (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross cut shredder and disposed of safely, in line with the VLC Data Security Plan.

6. Equipment and Digital Content

6.1 Personal mobile phones and mobile devices

- Mobile phones brought into VLC are entirely at the staff member, students & parents or visitors own risk. The VLC accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into Campus.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The VLC reserves the right to search the content of any mobile or handheld devices on the VLC premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the Campus, e.g. changing rooms and toilets.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The VLC strongly advises that student mobile phones should not be brought into the Campus.
- All students in years 2 – 8 in the Pupil Referral Unit should hand mobile phones and personally owned devices in at the office.
- Students in years 9 - 11 who bring mobile phones and personally owned devices must turn them off (not placed on silent) and store out of sight on arrival at the Campus. They must remain turned off and out of sight until the end of the day, unless in use for curriculum purposes.
- Where parents / carers or students need to contact each other during the Campus day, they should do so only through the Campus's telephone.
- The VLC 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 VLC policy then the phone or device will be confiscated and will be held in a secure place in the office. Mobile phones and devices will be released to parents or carers in accordance with the VLC policy.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone 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.

Staff use of personal devices

- Any permitted images or files taken in the VLC must be downloaded from the device and deleted before the end of the day.
- Staff are advised **not** to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a Campus phone where contact with students, parents or carers is required. In an emergency where a staff member does not have access to a VLC owned device, they should use their own device and withhold their own mobile number for confidentiality purposes.
- If a staff member is expecting a personal call they may leave their phone with the office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- 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 or for educational circumstances
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the VLC policy then disciplinary action may be taken.

6.2 Digital images and video

In the VLC:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the student VLC agreement form when their child joins the VLC;
- If specific student photos (not group photos) are used on the VLC web site, in the prospectus or in other high profile publications the VLC will obtain individual parental or pupil permission for its long term use
- We do not identify students in online photographic materials or include the full names of students in the credits of any published VLC produced video materials / DVDs;
- Staff sign the VLC's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- The VLC blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Students are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include management committee members, parents/carers or younger children as part of their ICT 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, such as house number, street name or the VLC. We teach them about the need to keep their data secure and what to do if they are subject to bullying, abuse or radicalisation.

6.3 Asset disposal

- Details of all VLC owned hardware will be recorded in a hardware inventory.
- Details of all VLC-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The VLC will only use authorised companies who will supply a written guarantee that this will happen
- 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.

APPENDIX 1

Voyage Learning Campus (VLC)
VLC Acceptable Use Policy for staff (including supply staff and volunteers where applicable)

Policy to be read in conjunction with the following document:

- ***VLC Safeguarding Policy***
- ***VLC Cyber bullying Policy***
- ***VLC Use of digital and video images Policy***
- ***VLC Electronic Devices – Searching and Deletion Policy***
- ***VLC Virtual Learning Environment (VLE) Policy***
- ***Hosted SIMS & SIMS Learning Gateway Policy***
- ***VLC Online Safety Policy***

1.1 This policy covers the use of digital technologies in the VLC: i.e. email, Internet network resources, learning platform, software, equipment and systems.

- I will only use the VLC's digital technology resources and systems for Professional purposes or for uses deemed reasonable by the Principal and the VLC Management Committee.
- I will not reveal my password(s) to anyone not authorised to access my account.
- I will follow advice in the creation and use of my password, which must include at least one lowercase letter, one uppercase letter, one number and one special character, and must be at least 8 characters long. 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 / network, or other school / LA systems.
- I will ensure all documents; data etc. are saved, accessed and deleted in accordance with the VLC's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any VLC business.
- I will only use the approved VLC email, school virtual learning environment (VLE) or other VLC approved communication systems with students or parents/carers, and only communicate with them on appropriate VLC business.
- I will use the VLC's VLE in accordance with the VLC Virtual Learning Environment (VLE) Policy and Campus protocols.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / VLC named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet 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, firewall and other ICT 'defence' systems.

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the VLC, is provided solely to support my professional responsibilities. I have read and signed (where relevant), the Portable Equipment Loan Policy.
- I will access VLC resources remotely (such as from home) only through the VLC approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow VLC Data Security Plan 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 student information, held within the Campus'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 understand that all Internet usage, network usage and emails can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-Campus safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff and Designated Safeguarding Lead at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action.
- I will not access inappropriate websites whilst using my Staff Proxy and understand that all web sites accessed and browsed by me will be logged against my name. I will therefore be held responsible for any web sites that I access.
- I must not divulge my Staff Proxy account to anyone and must ensure that students are not allowed onto a computer that is logged into my Staff Proxy.

VLC Acceptable Use Policy for Staff (including supply staff and volunteers where applicable)

Staff Agreement Form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date, read, and understand the school's most recent Online Safety policies.

I wish to have an email account; be connected to the Internet and be able to use the VLC's ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

School: Voyage Learning Campus

Authorised Signature: School Operations Manager

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

APPENDIX 2

Voyage Learning Campus
Acceptable Use Agreement Form
Key Stage 1

Think before you click

S

I will only use the internet and email with an adult

A

I will only click on icons and links when I know they are safe

F

I will only send friendly and polite messages

E

If I see something I don't like on a screen, I will always tell an adult

My Name: ……

My Signature:……

Voyage Learning Campus (VLC)
Acceptable Use Agreement Form
Key Stage 2

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

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

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

Signature : ……..

Full name : …….... (Printed)

Date : …….....

Voyage Learning Campus (VLC)
Acceptable Use Agreement Form
Key Stage 3 and Key Stage 4

- I will only use ICT systems in the VLC, including the Internet, email, digital video, mobile technologies, etc. for legitimate VLC purposes.
- I will not use my VLC email address to sign-up to any website, social media network or any other online service unless authorised to do so by VLC.
- I will not download or install software on Campus technologies.
- I will only log on to the school network/ Virtual Learning Environment with my own user name and password.
- I will follow the Campus ICT security system and not reveal my passwords to anyone and change them regularly.
- I will not use anyone else's username and password.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a Campus project approved by my teacher.
- Images of students and/ or staff will only be taken, stored and used for VLC purposes in line with VLC policy and will not be distributed outside the school network without the permission of the Principal.
- I will ensure that my online activity, both in the Campus and outside Campus, will not cause the VLC, the staff, students or others distress.
- My online activity both in the VLC and outside will not bring the VLC into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the Internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers and parents / carers.
- I understand that these rules are designed to keep me safe and that if they are not followed, VLC sanctions will be applied and my parent / carer will be contacted.
- I understand that I must use loaned equipment in line with the terms of the loan agreement form

Signature : ……..

Full Name : ……..... (Printed)

Date : …….....

APPENDIX 3

Voyage Learning Campus (VLC)

Record of Online Safety incidents (responding to incidents of misuse)

Details of all Online Safety incidents are to be recorded and reported to the Online Safety Co-ordinator. This log will be monitored termly by the Principal and members of the Senior Leadership Team. Any incidents involving cyber-bullying should also be recorded on this form.

Group	
Date/time	
Reason for investigation	

Details of first reporting person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web address / device misuse	**Reason for concern**

Conclusion and Action proposed or taken

This form should be returned to your head of centre once completed

Responding incidents of misuse – flow chart