CAPELLA HOUSE SCHOOL
E-SAFETY POLICY

The AURIGA Academy Trust Document Control System	
Name of document	E-Safety Policy
Status	Draft
Date Approved	
Approver	Pupil Achievement, Wellbeing and Safeguarding
Owner	Headteacher
Author	Lynn Majakas
Anticipated Review date	Annually
Location	Capella House School website.

Contents

Policy Overview

This e-safety policy has been developed by a working group made up of:

- School E-Safety Officers
- ICT Co-ordinators
- Headteacher and Senior Leaders
- Teachers
- Support Staff
- ICT and Online Safety Adviser
- ICT Technical staff
- Governors

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council input
- INSET sessions
- Governors meeting
- Parents workshops
- School communications, for example via the website and regular newsletters

Schedule for development, monitoring and review

This e-safety policy was approved by the Governors Committee on:	DATE TBC
The implementation of this e-safety policy will be monitored by the:	E-Safety committee, consisting of the E-Safety Co-ordinator ICT Co-ordinator Senior Leadership team
Monitoring will take place at regular intervals:	At this stage it is proposed that this will be on an annual basis; however, this will be reviewed and revised as and when necessary.
The Governors Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	At this stage it is proposed that this will be on an annual basis; however, this will be reviewed and revised as and when necessary.
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	DATE February 2020
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	ICT and Online Safety Adviser Police Commissioner's Office SPA

The school will monitor the impact of the policy using:

- Logs of reported incidents – see appendices
- Surveys / questionnaires of
- Pupils eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey
- Parents and carers
- Staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school 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 out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and will, where known, inform parents and carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors' Pastoral & Wellbeing Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding and *E-Safety Governor,* and this includes:

- regular meetings with the DSL and E-Safety Officers
- regular monitoring of e-safety incident logs
- regular monitoring of filtering and changing the control logs
- reporting to relevant Governors' committee

Headteacher and Senior Leaders

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety/ICT Co-ordinators.

- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety/ICT Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety/ICT Co-ordinator.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (Please see Capella House's flow chart on dealing with e-safety incidents).

E-Safety Coordinator

The role of the E-Safety Co-ordinator includes:

- taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- providing training and advice for staff
- liaising with the Local Authority
- liaising with school ICT technical support
- receiving reports of e-safety incidents and creating a log of incidents to inform future e-safety developments
- meeting regularly with E-Safety Governor to discuss current issues, review incident logs and filtering and changing control logs
- attending relevant Governors' meetings
- reporting regularly to Senior Leadership Team

ICT Technical Support

The E-Safety/ICT Co-ordinator is responsible for ensuring that the ICT Support provided by an outside contractor carries out e-safety measures in line with the school's and Auriga Academy Trust's policy, including:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- keeping up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant (See contract)

Teaching and Support Staff

Teaching and support staffs are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety/ICT Co-ordinator /Headteacher / Senior Leader / Class Teacher for investigation / action / sanction
- digital communications with students / pupils should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities

- students / pupils are supported to understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices; they monitor their use and implement current school policies with regard to these devices

Designated Safeguarding Lead

The DSL officer is trained in e-safety issues and aware of the potential for serious safeguarding and 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
- incitement to terrorism (see safeguarding policy)

Pupils

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they or their parents/ carers will be expected to sign before being given access to school systems.
- will be supported to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also be supported to know and understand school policies on the wide-ranging e-safety issues and the law in relation to these.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local e-safety campaigns and literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy**

Community Users

Community Users who access school ICT systems and the website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need

the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme provided as part of ICT / PSHE / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-safety messages will be reinforced as part of a planned programme of assemblies, tutorial and pastoral activities
- Pupils will be taught to be critically aware of the materials / content that they access on-line and be guided to validate the accuracy of information
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Education – parents and carers

Many parents and carers of pupils at Capella House have limited access to the Internet and a limited understanding of e-safety risks and issues. The school aims to provide on-going information and awareness to parents and carers through:

- Newsletters, letters and the website
- Parents evenings and workshops
- Reference to external e-safety third parties

Education and Training – Staff

All staff will receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training sessions – including regular audits of the e-safety training needs of staff.
- The E-Safety/ICT Coordinator will receive regular updates through attendance at LGfL/ LA/ other information and training sessions
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety/ICT Coordinator will provide advice / guidance / training as required to individuals

Training – Governors

Governors will take part in e-safety training / awareness sessions, for example via:

- Attendance at training provided by the Local Authority / National Governors Association and other relevant organisations.
- Participation in school training / information sessions for staff and parents

Technical – infrastructure / equipment, filtering and monitoring

It is the responsibility of the school and E-Safety/ICT Co-ordinator to ensure that their outside ICT support service contractor is up-to-date and carries out all the e-safety measures, and is

fully aware of the LGfL Security Policy and Acceptable Usage Policy. This includes ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented, where:

- The school ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the LGfL Security Policy and Acceptable Usage Policy and any relevant Trust E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems.
- All users will be provided with a username and password issued by LGfl and/or Trust systems
- The “master / administrator” passwords for the school ICT system is available to limited and named personnel and kept in a secure place.
- Users are responsible for the security of their own username and password and must immediately report any suspicion or evidence that there has been a breach of security.
- Requests from staff for sites to be removed from the filtered list are reported to the ICT Co-ordinator who reviews these and takes action when appropriate.
- An appropriate system is in place for users to report any actual / potential e-safety incidents to the ICT Co-ordinator, Headteacher or other members of the SMT (please see appendices for further details).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, temporary agency staff) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

- Where relevant E-safety will be a focus in all areas of the curriculum and staff will reinforce e-safety messages in the use of ICT across the curriculum.
- When using digital images, staff will inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images and the law. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.
- Staff must ensure that they:
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Unsuitable / inappropriate activities

Capella House School restricts internet usage in line with LGfl and the Trust guidelines.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

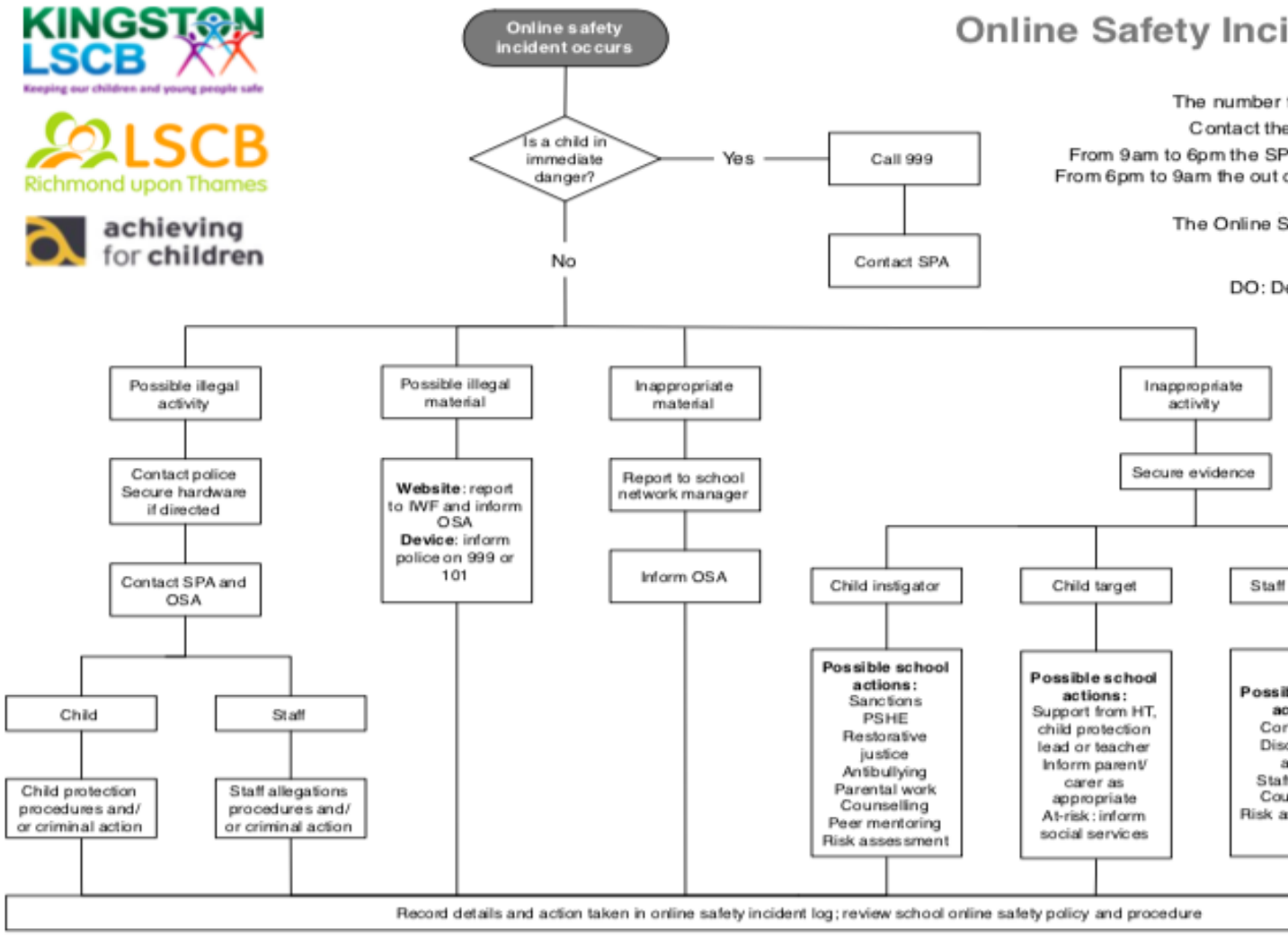
Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

the E-Safety and Designated Safeguarding Lead must be consulted **immediately** and actions followed in line with the E-Safety Incident Flow chart overleaf (as per the flow chart provided by AfC's ICT and Online Safety Adviser).

With incidents that involve inappropriate rather than illegal misuse, the incidents will be dealt with through Capella House's agreed Behaviour Policy.


KINGSTON LSCB
Keeping our children and young people safe
LSCB
Richmond upon Thames
achieving for children
Online safety incident occurs
Online Safety Inci
The number
Contact the
From 9am to 6pm the SP
From 6pm to 9am the out
The Online S
DO: D
Is a child in immediate danger?
Yes
Call 999
Contact SPA
No
Possible illegal activity
Contact police Secure hardware if directed
Contact SPA and OSA
Child
Staff
Child protection procedures and/ or criminal action
Staff allegations procedures and/ or criminal action
Possible illegal material
Website: report to IWF and inform OSA
Device: inform police on 999 or 101
Inappropriate material
Report to school network manager
Inform OSA
Inappropriate activity
Secure evidence
Child instigator
Child target
Staff
Possible school actions: Sanctions PSHE Restorative justice Antibullying Parental work Counselling Peer mentoring Risk assessment
Possible school actions: Support from HT, child protection lead or teacher Inform parent/ carer as appropriate At-risk: inform social services
Record details and action taken in online safety incident log; review school online safety policy and procedure

Appendices
Parents/Carers and Pupil Acceptable Use Policy Agreement
RULES FOR USING COMPUTERS and ELECTRONIC DEVICES

Electronic devices are here to help our learning. These rules will help us to keep safe.

Everyone must follow these rules.

When I am using computers I will:

- Always use them safely.
- Never use computers to hurt or bully anyone.
- Remember that everything I do on my computer can be seen.
- Only use my own password.
- Always keep my password safe.
- Not use anyone else's password or files or work.
- Not leave my computer open for others to use.
- Close a computer if I see it has been left open.
- Not put new programs on my computer.
- Log off the computer when I have finished.

I will tell a teacher if:

- I see any nasty or inappropriate pictures or messages.
- I see anything that makes me feel uncomfortable.
- There is a problem with a computer.

I will ask a teacher before:

- taking photographs or videos
- using my computer for games, music or videos
- copying anything to take out of school
- bringing my own programs, games or consoles to school

When I am sending messages I will:

- Only use my school email address
- Be polite, kind and responsible
- Not use personal equipment (e.g. mobile phones)
- Not pass on any chain letters

When I am on the Internet anywhere I will:

- Follow the SMART rules to keep safe online
- Not share personal information about myself or others
- Not use social networks or chat rooms when in the school.

Parent(s)/Carers(s)

- I have read and accept all of the above in support of and on behalf of my child.
- I will discuss Internet safety issues with my child.
- I will try to ensure that they are fully aware of the risks of Internet use and of school's Acceptable Use Policy.
- I accept that in accordance with 'Advice for Headteachers, School Staff and Governing Bodies - January 2018 Searching, Screening and Confiscation' the school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity has taken place.
- I understand that the school may contact the police as part of its responsibility under the Auriga Academy Trust's Child Protection Policy.
- I will NEVER UPLOAD photographs and/or videos of other children of Capella House School on to any website including any social media site such as Facebook, Twitter etc. without their permission.

Name of Pupil: _____ Class: _____

Signed by Pupil: _____(Year 6 and above)

Date: _____

Signed by Parent/Carer: _____

Date: _____

Staff (and Volunteer) Acceptable Use Policy (AUP)

Purpose of this Policy

Capella House School has provided ICT equipment for use by staff as an important tool for teaching, learning and administration. Use of the school's ICT systems, by both members of staff and pupils, is governed at all times by this policy. Please ensure that you understand your responsibilities under this policy and direct any questions or concerns to the ICT Coordinators in the first instance.

The purpose of this policy is to ensure that the school's ICT systems are operated safely and all users of ICT are safe. Further, it explains the behaviours that are acceptable and unacceptable.

This policy refers to our school's ICT network (server), domain (secure online area), all associated ICT services and to the use of mobile technologies within these.

Staff Responsibilities

All members of staff have a responsibility to use the school's ICT systems in a professional, lawful and ethical manner. This policy must be fully complied with at all times. All users of the school's ICT systems should note that our systems are monitored and logged. Any person found to have misused our systems or not to have followed this policy could face the following consequences:

- Temporary or permanent withdrawal from the school's ICT systems
- Suspension from duties and exclusion from the school site pending an investigation
- Disciplinary action
- In the most serious cases legal action may also be taken.

Whilst our ICT systems are organised to maintain the most secure environment possible ***it is the responsibility of all staff to make sure the pupils they are working with are safe***.

As an adult working in school, each member of staff may be the first point of contact in dealing with incidents of ICT misuse or abuse. Every such incident must be reported. All adults working in school must do so under the guidance of the member of staff to whom they are responsible.

With regard to e-safety and the acceptable use of ICT, staff must refer issues and incidents as follows:

- TAs, therapists and support staff to teachers
- Administration staff to the School Business Manager (SBM)
- Teachers, SLT and SBM to the ICT Coordinator
- ICT Coordinator to the Headship Team

Staff should report:

- Any websites accessible from within school that may not be suitable for staff or pupils.

- Any inappropriate content suspected to be stored on the school's ICT systems. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or
- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school's ICT systems.

The specific responsibilities of all staff:

- Developing and maintaining knowledge of Internet safety issues, particularly with regard to how they might affect children. Help, advice and resources are available through Childnet International: https://www.childnet.com/
- Maintaining an appropriate level of professional conduct in their own Internet use.
- Ensuring they have read the AUP for pupil use of ICT and that the pupils they work with adhere to this by:
    - Ensuring a copy of the AUP for pupils and SMART rules are displayed in each secondary pupil's planner.
    - Ensuring a copy of the SAFE Poster is visible in KS2 classrooms.
    - Reinforcing the AUP and SMART rules with pupils in their daily use of ICT.
    - Implementing the school's AUP through effective classroom practice.
- Supporting pupils who experience problems when using the Internet by working with the Class Teacher and the ICT coordinator.
- Using the Internet and ICT facilities to ensure that Internet safety is not compromised e.g. evaluating websites in advance of classroom use, using child-oriented search engines.
- Embedding Internet safety messages wherever possible.
- Following the school rules relating to acceptable use of our ICT equipment and other mobile technologies.
- Liaising with parents and the Designated Safeguarding Lead when necessary.

Passwords

The school operates a fully pass worded ICT system with individual accounts, there are no general user accounts issued and accounts are only issued for users on the school's MIS.

Each child and adult working within the school:

- Must log in to our ICT systems using the usernames and passwords given to them.
- Must keep their passwords secret.
- Is forbidden to use another person's account.
- Must, if they find an unattended machine logged on to another account log it off immediately.
- If they need to leave their computer, must lock it to prevent others from using their account.
- Must ensure that if someone has learned their password, they change it immediately (staff) or arrange with the ICT coordinator to have it changed (pupils). Please note that USO passwords must always be changed using the USO website.

For the children in our school who are unable to understand the pupils' AUP and for the children who are unable to log in and log off using their own password, the adult(s) working with those children will take full responsibility for their safe Internet use in school.

Software and Downloads

- Users must NOT use USB storage devices on the school's ICT systems until they have been virus checked and must take responsibility for ensuring this is done before connecting them. If in doubt consult our ICT Support Service or the ICT Coordinator.
- All users are prohibited from installing software onto the school's ICT systems except in the following case: staff may add apps and chrome extensions to their own Chromebooks for use in their work and to trial for possible use by students.
- If domain or network users need a new program, app or extension, this will be installed by the school's ICT support service if possible.
- Copyright and intellectual property rights must be respected when downloading from the Internet.

Personal Use

The school recognises that occasional personal use of the school's ICT systems is beneficial both to the development of ICT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use:

- Must comply with this AUP and all other school policies regarding staff conduct.
- Must not interfere in any way with individual staff duties or those of any other member of staff.
- Must not have any undue effect on the performance of our ICT systems.
- Must not be for any commercial purpose or gain unless explicitly authorised by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

Email

- All users are issued with a school email address for communication both internally and with email users outside of the school.
- No member of staff (including governors and non-teaching staff) must use non-school email accounts for any school or work related activity – no exceptions.
- Pupils are not permitted under any circumstances to email a member of staff using their personal email address and members of staff must not email pupils using their personal email address.

- Users are responsible for email they send and should be aware that these are open to be read and should be treated as public.
- All staff must remember they are representative of the school on a global public system.
- Emails must be written carefully and the content should:
    - use appropriate and respectful language, be polite and never contain anything that is likely to cause needless anxiety
    - not use language calculated to incite hatred against ethnic, religious or other minority.
- Any unsuitable communication received must be reported immediately to the ICT Coordinator or a member of the headship team.
- Anonymous messages and chain letters must not be sent.
- Email attachments should only be opened if the source is known and trusted.
- Illegal activities of any kind are strictly forbidden and messages relating to or in support of illegal activities will be reported to the police.

Personal Information

- Staff will not reveal any personal information of other users to any unauthorised person (e.g. name, address, age, telephone number, social network details).
- Staff will not reveal any of their personal information to pupils.
- When working with personal data, staff will check and ensure that the data is secure.

Images/Videos

- No images of pupils can be taken without:
    - Parental consent, which is recorded on the school's MIS.
    - Permission from a member of the teaching staff to use any school mobile device such as iPods, phones, Chromebooks and school cameras.
- All children need parental permission for photographs or videos to be published electronically or in a public area even if they are unidentifiable.
- No photos or videos which include nudity or inappropriate actions are permitted to be taken or downloaded under any circumstance.
- It is forbidden to take photographs or videos of pupils on a personal mobile phone, excepting only where the Uploadcam Android App is used, which must be installed and logged into the school's secure domain before any video or photograph is taken.
- It is forbidden for staff to keep any video or image of a pupil on their mobile phone.

ICT Systems Protocol

- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- School ICT and Internet use must be appropriate to a pupil's education and maturity or to staff professional activity.
- All users will not trespass into other users' files or folders.

- All users will respect other's data and work, and not corrupt, interfere with or destroy them.
- Staff have a duty to ensure that these protocols are enforced with pupils.

Internet Usage

- Pupils must be supervised at all times when using the Internet.
- Activities should be planned so open searching is kept to a minimum.
- When searching the Internet with pupils, adults should encourage the pupils to use 'child safe' search engines. However, safe search and filtering for pupils is set on ICT systems as a default.
- The use of social networking sites, public chat rooms and messaging systems (Facebook, Messenger, Twitter...) is not allowed in school, excepting those that are provided by G Suite on the school's secure domain.
- Staff may not use the school's Internet connection for personal financial gain, gambling, political purposes and advertising all of which is forbidden.
- Staff will not attempt to visit websites that may be considered inappropriate or illegal.
- Staff must be aware that downloading some material is illegal and that the police or other authorities may be called to investigate.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time and on their own computer. Social Networking sites invite users to participate in informal ways that can leave staff open to abuse, and often make little or no distinction between adult users and children.

In your own social networking online, you must:

- Not allow any pupil to access personal information you post on a social networking site.
- Not add a pupil to your Friends list, neither must you invite them to be friends with you.
- Ensure that personal information is not accessible via a Public setting.
- Avoid contacting any pupil privately via social networking site, even for school-related purposes.
- Take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.

Staff are advised not to agree to requests from the pupils' parents or carers to add them as a friend to their social networking sites, nor should you invite them to be your friends. Damage to professional reputations can inadvertently be caused by quite innocent postings or images. Staff will need to ensure that any private social networking sites and blogs that they create or actively contribute to are not to be confused with their professional role in anyway.

Staff should also take care when posting to any public website, including online discussion forums or blogs, that their comments do not harm their professional standing or the reputation of the school, even if their online activities are entirely unrelated to the school.

In particular, staff must not:

- Post comments on websites that may appear as if you are speaking for the school, unless authorised to do so.
- Post any material online that can be clearly linked to the school and that may damage the school's reputation.
- Post any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own equipment

- Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) and must not be used until approved.
- Staff must not connect personal computer equipment to the school's ICT systems without prior approval from ICT Coordinator.

Staff Mobile Devices

- During the school day, staff mobile phones must be turned off or put on silent mode and kept out of sight of pupils.
- Staff are allowed to access their personal phones on breaks, lunch times and after school in suitable areas e.g. staffroom or workroom; places where the pupils are not present.
- Staff must ensure that calls, ringtones, alarms and notifications are not audible at meetings and do not interrupt the business of the school.

Supervision of Pupils

- Pupils must be supervised at all times when using the school's ICT systems.
- When arranging use of ICT for pupils, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the AUP for pupils is enforced.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this AUP is followed. They must immediately inform the ICT Coordinator or the Head of Centre of abuse of any part of the ICT system. In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the school's ICT system. This may be contained in email, documents, pictures, etc.
- Any breaches, or attempted breaches, of computer security, or

- Any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school's ICT system.

All reports will be treated confidentially.

Electronic Devices - Searching & Deletion

In accordance with 'The Education Act 2012' the school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity has taken place. (See 'Advice for Headteachers, School Staff and Governing Bodies - January 2018 Searching, Screening and Confiscation').

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure.

School Filtering Policy

Introduction
As a part of the LGfl, Capella House automatically receives the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities
The responsibility for the management of the school's filtering policy is held by the E-Safety/ICT Co-ordinators. They will manage the school filtering, in line with this policy and will keep records of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the E-Safety/ICT Co-ordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Education / Training / Awareness
Pupils will be made aware of the importance of filtering systems through the ICT and e-safety curriculum.
Staff users will be made aware of the filtering systems through staff meetings, briefings and communications.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions and regular communications such as the website and newsletters.

Changes to the Filtering System
The form overleaf needs to be completed by a user requesting changes to the filtering system, and this is subsequently reviewed and agreed or denied by the E-Safety/ICT Co-ordinator and DSL.

Audit / Reporting
Logs of filtering change controls and of filtering incidents will be made available to:
- the Designated Safeguarding Lead
- E-Safety/ICT Co-ordinator
- LGfl / The Auriga Academy Trust on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.