CHELSEA ACADEMY

Anchored in Christ

Electronic Information and Communications Systems Policy

Approved by Governor committee:
N/A

Date to be reviewed:
Summer 2024

Responsibility of :
Director of Finance and Operations

Date ratified by Principal:
Principal - LT meeting 24th May 2022

1. General Statement **4**

2. Key responsibilities of the community **4**
2.1 Key responsibilities of the Principal 4
2.2 Key responsibilities of the DFO 5
2.3 Key responsibilities of the Network Manager 5
2.4 Key responsibilities of all staff 5
2.5 Key responsibilities of all students 6
2.6 Key responsibilities of the Parents and Carers 6

3. The Academy network **6**
3.1 Policy and procedures 7

4 Managing the network and Equipment **8**
4.1 Using the Academy network, equipment and data safely: general guidance 8
4.2 Policy / Procedure statements 8

5. Use of Technology **10**
5.1 Internet Filtering 10
5.2 Email Filtering 10
5.3 Encryption 10
5.4 Passwords 10
5.5 Anti-Virus 11

6 Online communication **11**
6.1 Internet 11
6.2 Email 11
6.3 Publishing of Photos and videos 12
6.4 Social Networking 12
6.4.1 General social media use 12
6.4.2 Staff official use of social media 13
6.4.3 Staff personal use of social media 13
6.4.4 Students use of social media 14
6.5 Use of Personal Devices and Mobile Phones 14
6.5.1 Expectations for safe use of personal devices and mobile phones 14
6.5.2 Staff use of personal devices and mobile phones 15
6.5.3 Students use of personal devices and mobile phones 15
6.6 Training and Curriculum 16

7. Data Security **16**
7.2 Handing Infringements 17
7.3 Informing staff and students of these procedures 17

8. Management of applications (apps) used to record students' progress **17**

9. Responding to Online Incidents and Concerns **18**

Appendix A Student Acceptable Use Policy (AUP) **19**

Appendix B Staff Acceptable Use Policy **20**

Appendix C Staff Laptop Acceptance Form **22**

1. General Statement

At Chelsea Academy we believe that online safety (e-Safety) is an essential element of safeguarding students and adults in the digital world when using technology such as computers or mobile phones. The Academy identifies that internet and information communication technologies are an important part of everyday life so students must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

The Academy has a duty to provide the Academy community with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the Academy management functions. The Academy also identifies that within this there is a clear duty to ensure that students are protected from potential harm online.

The purpose of this Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the Academy is a safe and secure environment.
- Safeguard and protect all members of the Academy community online.
- Raise awareness with all members of the Academy community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with Academy issued devices for use off-site, such as a work laptop or mobile phone.

For clarity, this policy uses the following terms unless otherwise stated:

- Users - refers to teachers, support staff, governing board, academy volunteers, students and any other person working in or on behalf of the academy, including contractors.
- Parents – any adult with a legal responsibility for the child/young person outside the academy e.g. parent, guardian, carer.
- Academy – any Academy business or activity conducted on or off the Academy site, e.g. visits, conferences, academy trips etc.

2. Key responsibilities of the community

2.1 Key responsibilities of the Principal

The Principal has overall responsibility for e-Safety within the Academy. The day-to-day management of this will be delegated to the Director of Finance and Operations (DFO). The DFO will:

- Deliver e-Safety training throughout the Academy and ensure that it is planned well, is progressive and up to date and appropriate to the recipient, (i.e. students, all staff, senior leadership team, governing body, and parents).
- Have had appropriate CPD in order to undertake their day-to-day duties.
- Ensure all e-safety incidents are dealt with promptly and appropriately.
- Keep up to date with emerging risks and threats through technology use

2.2 Key responsibilities of the DFO

- Review this policy annually and in response to any significant e-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the Academy and to ensure e-safety incidents are appropriately dealt with. They will also review the policy so that it is effective in managing those incidents
- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for Academy and home use.
- Advise the Academy on all e-safety matters.
- Engage with parents and the community on e-safety matters.
- Liaise with the local authority, Network Manager and IT technical support and other agencies as required.
- Retain responsibility for the e-safety incident log; ensure staff understand what to report and ensure the appropriate audit trail.
- Ensure any technical e-safety measures in the Academy (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the governors and Network Manager.
- Make themselves aware of the technical e-safety reporting functions available.

2.3 Key responsibilities of the Network Manager

- The IT technical infrastructure is secure; this will include as a minimum:
    - Antivirus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any e-safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the DFO, and approved by the Leadership Team (LT).
    - Passwords are applied correctly to all stakeholder users regardless of age.
    - Clear responsibilities for the daily backup of MIS and finance systems and other important files;

2.4 Key responsibilities of all staff

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the DFO.
- Any e-safety incident is reported to the DFO and Pastoral team (and an e-Safety Incident report is made), or in his/her absence to the Principal. If you are unsure, the matter is to be raised with the DFO or the Principal to make a decision.
- The reporting flowcharts contained within this policy are fully understood.
- Reading the Academy's Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of Academy/ systems and data.
- Having an awareness of online safety issues, and how they relate to the children in their care.
- Embedding online safety education in curriculum delivery wherever possible.
- Identifying individuals of concern, and taking appropriate action by working with the DFO.
- Knowing when and how to escalate online safety issues, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

2.5 Key responsibilities of all students

The conditions of use of ICT equipment and services in this Academy are given in the student Acceptable Use Policy (see Appendix A); any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at Academy or outside of Academy.

- Reading the Academy's Acceptable Use Policies (AUPs) and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

2.6 Key responsibilities of the Parents and Carers

Parents play the most important role in the development of their children; as such the Academy will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the Academy environment. Through parent consultation evenings and half termly newsletters the academy will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

- Reading the Academy's AUPs, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the Academy in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the Academy, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Contributing to the development of the Academy's online safety policies.
- Using the Academy's systems, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

3. The Academy network

- Has filtered secure broadband connectivity through the London Grid for Learning (LGfL) Uses the LGfL filtering system to block sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Uses USO filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;.
- Ensures network health through use of Microsoft Defendersoftware and Sophos antivirus and network set-up so staff and students cannot download/install executable files;

- Uses individual, audited logins for all users ;
- 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 / Internet Literacy lessons;
- Only uses approved or checked webcam sites;
- Has 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;
- Uses security time-outs on Internet access where practicable / useful;
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Has additional local network auditing software installed; 'Impero Education Pro'
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;

3.1 Policy and procedures

The Academy:

- 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 the appropriately secure Academy's learning environment;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the Academy's Learning Platform as a key way to direct students to age / subject appropriate web sites;
- Plans the curriculum context for Internet use to match students' ability;
- Never allows / Is vigilant when conducting 'raw' image search with students e.g. Google or Lycos image search;
- Informs users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the IT Manager or system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL (Atomwide) as necessary;
- Requires students to individually sign an acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an acceptable use agreement form and keeps a copy on file;
- Ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the Academy;
- 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;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the Academy behaviour management system;
- Ensures the named Designated Safeguarding Lead has appropriate training;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for

students, staff and parents
- Provides E-safety advice for students, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

4 Managing the network and Equipment

4.1 Using the Academy network, equipment and data safely: general guidance

Anyone providing personal data or sensitive personal data will know how their data will be used and shared. A copy of the Privacy Policy will be published on the Academy website, and can be found at Annex B to the Data Management and Protection Policy. All staff will confirm that they have read, understood and will abide by this policy. To ensure that processing is fair and lawful it will be done in accordance with one of the following grounds in the Act:

- The individual has given his or her consent
- The processing is necessary for the performance of a contract with the individual
- The processing is required under a legal obligation to which Chelsea Academy is subject
- The processing is necessary to protect the vital interests of the individual
- The process is necessary to carry out public functions
- The processing is necessary in order to pursue the legitimate interests of the Academy or third parties provided that that is balanced against the rights, freedoms and legitimate interests of the data subject
- The processing of sensitive personal data can only be carried out if one of the following additional conditions is also met (in addition to the conditions for processing set out above):
- The explicit consent, in writing, of the individual is obtained
- The data is required by law for employment purposes or the administration of justice or legal proceedings
- The processing is necessary for protection of the vital interests of the data subject or another
- The individual has already deliberately made the information public
- The processing is necessary for medical purposes, and undertaken by a health professional or someone who is subject to an equivalent duty of confidentiality
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of the individual.

The computer system / network is owned by the Academy and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The Academy reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

4.2 Policy / Procedure statements

To ensure the network is used safely this Academy:

- Ensures staff read and sign that they have understood the Academy's e-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.

- Controls staff access to the academy management information system through a separate password for data security purposes;
- Provides students with an individual network login username.
- Provides all students with their own unique username and password which gives them access to the internet, the Learning Cloud and their own Academy approved email account;
- 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;
- Makes it 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;
- Requires that where a user finds a logged-on machine, they 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.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- 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 Academy provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used solely to support their professional responsibilities and that they notify the Academy of any “significant personal use” as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed; e.g. projector filters cleaned by IT Support Team ; equipment installed and checked by approved Suppliers / LA electrical engineer
- 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; e.g. teachers access report writing module; SEN coordinator - SEN data;
- Ensures that access to the Academy’s network resources from remote locations by staff is restricted and access is only through Academy / LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support, parents using a secure portal to access information on their child;
- Provides students and staff with access to content and resources through the Learning Cloud which staff and students access using their username and password.
- Has a clear disaster recovery system in place for critical data that includes a secure, remote backup of critical data, that complies with external Audit’s requirements;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Ensures that all student level data or personal data sent over the Internet is encrypted;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Ensures our wireless network has been secured to Enterprise security level standards suitable for educational use;
- Installs all computer equipment professionally and meets health and safety standards;

- Maintains all projectors so that the quality of presentation remains high;
- Reviews the Academy ICT systems regularly with regard to health and safety and security.

5. Use of Technology

In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

5.1 Internet Filtering

At the Academy we use Atomwide software through the London Grid for Learning platform that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The DFO and Network Manager are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal.

In conjunction with the LGfL filtering we also have a proxy (Smoothwall) server that provides real-time filtering to prevent inappropriate content and enhance online protection. We are also able to see detailed data including internet usage, bandwidth & content categorisation. Flexible policies enable staff and students to be able to visit non-educational sites without compromising security.

We also use Impero Education Pro software with active monitoring and logging incident captures to provide contextual insight, helps the academy to identify potential risks, respond before an incident escalates, and educate students about responsible online behaviour. Furthermore, this classroom monitoring software empowers teaching staff with a range of classroom control, instruction and monitoring tools to help break down traditional behaviour management barriers, focus student learning, and keep young people safe.

5.2 Email Filtering

At the Academy our mail service is provided by Google for Education. Aggressive filters have been implemented to ensure that staff and students are protected both within the organisation and out. Custom objectionable words are defined so that inappropriate emails are monitored and/or blocked. Spam and phishing filters ensure that users don't receive suspicious emails that could deceive users into buying products and sharing their personal information (bank details, address, etc).

5.3 Encryption

All Academy portable devices that hold personal data (as defined by the Data Protection Act 2018) are encrypted. No data is to leave the Academy on an unencrypted device; all devices that are kept on Academy property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop) is to be brought to the attention of the Director of Finance and Operations immediately. The Director of Finance and Operations will decide whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

5.4 Passwords

All staff and students will be unable to access any device without a unique username and password. We encourage staff and students to change their passwords on a termly basis or if there has been a compromise, whichever is sooner. The DFO and IT Support will be responsible for ensuring that passwords are changed. New users are given at least an eight character long password consisting of upper/lower case letters, numbers and symbols. A policy has been implemented so that this complexity of password must be adopted

by all users.

5.5 Anti-Virus

All capable devices will have Microsoft Defender Protection software installed. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the DFO if there are any concerns.

6 Online communication

6.1 Internet

Use of the Internet in Chelsea Academy is a privilege, not a right. Internet use will be granted:

- to staff upon signing this e-safety and the staff Acceptable Use Policy;
- to students upon signing and returning their acceptance of the Acceptable Use Policy.

6.2 Email

All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. The following conditions apply to all members of staff:

- Staff should only use work email systems for professional purposes;
- Access in the academy to external personal email accounts may be blocked.
- Staff should be aware that email sent to an external organisation must be written carefully and may require authorization, in the same way as a letter written on Academy headed paper. It should follow the Academy 'house-style':
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the Academy must immediately tell a designated member of staff if they receive offensive communication. This person is the Senior Vice Principal (Inclusion) or the Principal.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- 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 emails is not permitted;
- Embedding adverts is not allowed.
- Academy email addresses and other official contact details will not be used for setting up personal social media accounts.

Students are permitted to use the Academy email system, and as such will be given their own email address. Students are introduced to, and use email as part of the ICT scheme of work; an important element of this is empowering 'good netiquette'. In particular students are taught:

- Not to give out their email address unless it is part of a Academy managed project, or to someone they know and trust and is approved by their teacher or parent/carer;
- That an e-mail is a form of publishing where the message should be clear and concise;
- That any email sent to an external organization should be written carefully and authorized before sending, in the same way as a letter written on Academy headed paper;
- They must not reveal private details of themselves or others in email, such as address, telephone number, etc;
- To 'Stop and Think Before They Click' and not open attachments unless they are sure the source

is safe;
- That they should think carefully before sending any attachments;
- Embedding adverts is not allowed;
- That they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages;
- Not to delete malicious of threatening emails, 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.
- Whole class or group emails will be blocked for students unless authorised by a senior member of staff.

6.3 Publishing of Photos and videos

The taking, and use, of student images will only be undertaken with full parental and student permission (which is taken on transition as part of the Home-Academy Agreement). Every precaution will be taken to ensure that names and photographs do not appear together; storage of this data is secure and only used by those authorised to do so.

6.4 Social Networking

6.4.1 General social media use

There are many social networking services available; Chelsea Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider Academy community. The following social media services are permitted and have been appropriately risk assessed:

- Blogging – used by staff and students in the Academy.
- Twitter – used by the Academy as a broadcast service (see below).
- A broadcast service is a one-way communication method in order to share Academy information with the wider Academy community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

Should staff wish to use other social media, permission must first be sought via the DFO who will advise the Principal for a decision to be made. Any new service will be risk assessed before use is permitted.

In addition, the following is to be strictly adhered to:

- Parental consent for photographs must be checked on SIMS before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the Academy are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).
- Notice and takedown policy – should it come to the Academy's attention that there is a resource which has been inadvertently uploaded, and the Academy does not have copyright permission to use that resource, it will be removed within one working day.

6.4.2 Staff official use of social media

- Staff using social media for educational/work purposes will disclose their official role/position but always make it clear that they do not speak on behalf of the Academy.
- Staff using social media for educational/work purposes will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- Staff using social media for educational/work purposes will always act within the legal frameworks they would adhere to within the academy, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Staff must ensure that any image posted on the Academy's social media platform have appropriate written parental consent.
- Staff using social media for educational/work purposes will be accountable and must not disclose information, make commitments or engage in activities on behalf of the academy unless they are authorised to do so.
- Staff using social media for educational/work purposes will inform their line manager, the Academy's online safety (e-Safety) lead and/or the Principal of any concerns such as criticism or inappropriate content posted online.
- Staff will not engage with any direct or private messaging with students or parents/carers through social media and should communicate via the academy's communication channels.

6.4.3 Staff personal use of social media

The expectations of staff are outlined in the Academy code of conduct and these should be followed. The information below is an addition to this guidance.

- Academy staff will not invite, accept or engage in communications with parents or children from the Academy community in any personal social media whilst in employment at Chelsea Academy.
- Any communication received from children on any personal social media sites must be reported to the designated person for Child Protection.
- Staff must be vigilant and if they are aware of any inappropriate communications involving any child in any social media, these must immediately be reported.
- Members of the Academy staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the Academy community on Academy business must be made from an official Academy email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the Academy community on Academy business, nor should any such contact be accepted, except in circumstances given prior approval by the Principal.
- Staff are advised to avoid posts or comments that refer to specific, individual matters related to the Academy and members of its community on any social media accounts.
- Staff are also advised to consider the reputation of the Academy in any posts or comments related to the Academy on any social media accounts.
- Staff should not accept any current student of any age or any ex-student of the Academy under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Staff should ensure that any dating apps are used carefully and that current or past students and parents are not contacted through them.

6.4.4 Students use of social media

- Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, Academy attended, Instant messenger contact details, information through photographs, email addresses, full names of friends/family, specific interests and clubs etc.
- Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with students and written parental consent will be obtained, as required.
- Any official social media activity involving students will be moderated by the Academy where possible.
- The Academy is aware that many popular social media sites state that they are not for children under the age of 13, therefore the Academy will not create accounts within Academy specifically for children under this age.
- Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at Academy, will be dealt with in accordance with existing the academy's policies including anti-bullying and behaviour. Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites.

6.5 Use of Personal Devices and Mobile Phones

6.5.1 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought into the Academy are the responsibility of the individual at all times. The Academy will not be held liable for the loss, theft or damage of such items. Nor will the Academy accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and personal devices are not permitted to be used in certain areas within the premises such as classrooms, changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the Academy and any breaches will be dealt with as part of the Academy's discipline/behaviour policy.
- Members of staff will be issued with an Academy telephone number/extension (if necessary) and email address where contact with students or parents/carers is required.
- Academy mobile phones and devices must always be used in accordance with the AUP
- Academy mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

Some members of staff will have Academy mobiles issued to them. The purpose of these mobiles is to ensure that key staff can be contacted throughout the day and can respond to parents during normal working hours. Holders of mobile phones should ensure that:

- Mobiles are looked after and secured when not in use.
- Mobiles are only used for work purposes.
- Students should only be able to use the academy mobiles if supervised by the member of staff who is responsible for them.
- If an academy phone is lost or stolen the Director of Finance and Operations must be told immediately.

Damage to academy mobile phones (if caused deliberately or through lack of care) will be the responsibility of the staff member to correct.

Academy phones can be used to take pictures of students on academy events.

6.5.2 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of the Academy in a professional capacity. Any pre-existing relationships which could compromise this must be discussed with the Principal.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose. Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be switched off/switched to ‘silent’ mode during lesson times.
- Bluetooth or other forms of communication should be “hidden” or switched off during lesson times.
- Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of LT in emergency circumstances.
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches the Academy’s policy then disciplinary action will be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted and allegations will be responded to following the Allegations of Abuse Against Staff policy.

6.5.3 Students use of personal devices and mobile phones

- Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- Mobile phones and personal devices will be switched off and kept out of sight.
- Mobile phones or personal devices will not be used by students during lessons or throughout the Academy day unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If a student needs to contact his/her parents/carers they will be allowed to use an Academy phone at students services or reception.
- Parents are advised not to contact their child via their mobile phone during the Academy day, but

to contact reception. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Head of Year and/or the Principal.

- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student breaches the Academy's policy then the phone or device will be confiscated and will be held in a secure place. Mobile phones and devices will be released to parents/carers in accordance with the Academy's policy.
- Academy staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the Academy's behaviour or bullying policy. The phone or device may be searched by a member of LT with the consent of the student or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the Academy's policy.
- If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

6.6 Training and Curriculum

● It is important that the wider Academy community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such we will have an annual programme of training which is suitable to the audience.

● e-Safety for students is embedded into the curriculum; whenever ICT is used in the Academy, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

● As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

● The DFO is responsible for recommending a programme of training and awareness for the Academy year to the Principal and responsible Governor for consideration and planning.

● Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Principal for further CPD.

7. Data Security

7.1 Data security best practice guidelines

Passwords - Do

● Use a strong password (strong passwords are usually eight characters or more and contain upper and lower case letters, as well as numbers).

Passwords - Don't

● Ever share your passwords with anyone else or write your passwords down.

● Save passwords in web browsers if offered to do so.

Laptops - Do

● Try to prevent people from watching you enter passwords or view sensitive information.

● Log-off / lock your 'desktop' when leaving your PC or laptop unattended.

Sending and sharing - Do

● Be aware of who you are allowed to share information with. Check with your Information Asset Owner(s) if you are not sure.

● Only use encrypted removable media (such as encrypted USB pen drives) if ever taking any 'Protected' data outside your Academy.

Sending and sharing - Don't

● Send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives), if secure remote access is available.

● Send sensitive information by email unless it is encrypted; student data must be sent via S2S (DCSF secure web site).

Working on-site - Do

● Lock sensitive information away when left unattended, i.e. in lockable drawers, log off or lock workstation.

Working on site - Don't

● Let strangers or unauthorised people into staff areas.

● Position screens where they can be read from outside the room.

Working off-site - Do

● Only take off site information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above.

● Wherever possible access data remotely instead of taking it off-site - using approved secure authentication.

● Make sure you sign out completely from any services you have used.

● Ensure you save to the appropriate area to enable regular

7.2 Handing Infringements

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the Academy management and will reflect the Academy's behaviour and disciplinary procedures. The staff code of conduct, home Academy agreement and disciplinary policy outline what is expected from staff and the consequences of not following Academy policy.

7.3 Informing staff and students of these procedures

They will be fully explained and included within the Academy Acceptable Use Policy. All staff will be required to sign the Academy acceptable use agreement form;

- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Students will sign an acceptable use agreement form;
- These procedures will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the Academy.
- Information on reporting abuse / bullying etc will be made available by the Academy for students, staff and parents.

8. Management of applications (apps) used to record students' progress

- The Principal is ultimately responsible for the security of any data or images held of students.

- Apps/systems which store personal data will be risk assessed prior to use.
- Personal staff mobile phones or devices will not be used for any apps which record and store students' personal details, attainment or photographs.
- Only Academy issued devices will be used for apps that record and store students' personal details, attainment or photographs.
- Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- Staff and students will be advised on safety measures to protect all members of the academy such as using strong passwords, logging out of systems, not sharing personal information, etc.

9. Responding to Online Incidents and Concerns

- Complaints about Internet misuse will be dealt with under the Academy's complaints procedure.
- Complaints about online bullying will be dealt with under the Academy's Anti-bullying Policy and procedure.
- Any allegations against a member of staff's online conduct will be handled under the Academy's Safeguarding, Code of Conduct and Disciplinary policies.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the Academy will need to be aware of the importance of confidentiality and the need to follow the official Academy procedures for reporting concerns.
- After any investigations are completed, the Academy will debrief, identify lessons learnt and implement any changes as required.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- If an incident of concern needs to be passed beyond the Academy then the concern will be escalated to the Education Safeguarding Team to communicate to other academies/settings in Kensington and Chelsea.

Appendix A Student Acceptable Use Policy (AUP)

This agreement is in place to ensure data integrity and personal responsibility when using ICT systems. The AUP is loaded on all computers and users will need to digitally sign the agreement upon login. The digital signatures are kept centrally by the IT service desk. In addition to this the AUP is also available in student planners.

Note: All Internet and network usage is automatically monitored.

1. I will only use the Academy's computers for Academy work and homework.
2. I will only edit or delete my own files and not look at, or change, other people's files without their permission.
3. I will keep my logins and passwords secret.
4. I will not bring files into the Academy without permission or upload inappropriate material to my workspace.
5. I will not attempt to visit Internet sites that I know to be banned by the Academy.
6. The use of social networking sites on Academy ICT equipment is not allowed unless specifically authorised by a member of staff as part of the planned curriculum.
7. I will only e-mail people I know, or a responsible adult has approved.
8. The messages I send, or information I upload, will always be polite and sensible.
9. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
10. 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.
11. 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.
12. I understand all the points above and agree to abide by them. Failure to comply with this AUP will result in sanctions as detailed in the Behaviour Policy.

Appendix B Staff Acceptable Use Policy

At Chelsea Academy we support the rights of all members of the Academy community to be provided with, and engage in a safe, inclusive and supportive learning environment. This extends to the use of digital tools and online communities and is underpinned by our expectation of safe and responsible behaviour of all members of the Academy community.

This AUP covers use of digital technologies in Academy: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems. You must read and agree to this policy before signing into the Academy network.

1. I will only use the Academy's digital technology resources and systems for professional, educational purposes or for uses deemed 'reasonable' by the Principal and Governing Board.
2. I will not reveal my password(s) to anyone.
3. I will follow 'good practice' advice in the creation and use of my password. If my password is compromised I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
4. I will not allow unauthorised individuals to access email / Internet / intranet / network, or other Academy systems.
5. I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the Academy's network and data security and confidentiality protocols.
6. I will not engage in any online activity that may compromise my professional responsibilities.
7. I will only use the approved, secure email system for Academy business.
8. I will only use the approved Academy email, Academy Learning Platform or other Academy approved communication systems with students or parents/carers, and only communicate with them on appropriate Academy business.
9. I will not browse, download or send material that could be considered offensive to members of the organisation.
10. I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Director of Finance and Operations and the Network Manager.
11. I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
12. I will not publish or distribute work that is protected by copyright.
13. 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 Academy's recommended anti-virus, firewall and other IT 'defence' systems.

14. I will not use personal digital cameras or camera phones for taking and transferring images of students or staff without permission and will not store images at home without permission.

15. I will use the Academy's Learning Platform in accordance with Academy protocols.

16. I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my role.

17. I agree and accept that any computer or laptop loaned to me by the Academy, is provided solely to support my professional responsibilities and that I will notify the Academy of any "significant personal use" as defined by HM Revenue & Customs.

18. I will access Academy resources remotely (such as from home) only through the LGfL / Academy approved methods and follow e-security protocols to access and interact with those materials.

19. I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Academy data security protocols when using any such data at any location.

20. I understand that data protection policy requires that any information seen by me with regard to staff or student information, held within the Academy'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.

21. I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.

22. I understand that electronic communications created, sent or received using Chelsea Academy email systems are the property of Chelsea Academy, and may be accessed by an Authorised Person in the case of an investigation, including in relation to investigations following a complaint or investigations into misconduct. Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on computer, including emails, may be accessible under the Freedom of Information Act 1982 (Vic). Please note that email messages may be retrieved from backup systems and organisations, their employees and the authors of electronic communications can been held liable for messages that have been sent.

23. We process all requests in accordance with data protection laws.

24. Chelsea Academy resources may be accessed or monitored by Administrators at any time without notice to the user. This includes, but is not limited to, use of Chelsea Academy email systems and other electronic documents and records.

25. Administrators may access or monitor the records of Chelsea Academy resources for operational, maintenance, compliance, auditing, legal, security or investigative purposes.

26. Users are only able to access their own profile and nobody else's unless specific arrangements have been made to monitor emails for example during long-term absence. Information on such access is privileged and available only to the Principal upon request.

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

Appendix C Staff Laptop Acceptance Form

Part of Chelsea Academy Improvement Plan is to provide laptop computers to Teaching staff to assist in the delivery of the Curriculum. The Principal has agreed that a laptop computer will be loaned to you while you remain employed at this Academy. This loan is subject to review on a regular basis, and can be withdrawn at any time.

As a member of staff to whom a laptop has been loaned I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

1. The laptop/device is for the work related use of the named member of staff to which it is issued.
2. Only software installed at the time of issue or software purchased by and licensed to Chelsea Academy may be installed on the machine.
3. The laptop/device remains the property of Chelsea Academy throughout the loan period. However, the member of staff to which is issued, will be required to take responsibility for its care and safe keeping.
4. If left unattended the laptop/device should be in a locked room or secure area.
5. Due regard must be given to the security of the computer if using other forms of transport.
6. In order to ensure the Academy's compliance with the Data Protection Act and to avoid breaches of confidentiality: under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from Academy particularly with files which may contain personal student data.
7. The laptop/device will be recalled from time to time for maintenance / upgrade and monitoring.
8. Should any faults occur, I agree to notify the Academy's ICT staff as soon as possible so that they
9. may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware, or any other faults.
10. I agree to attend training in how to access the Curriculum Network, Intranet, Internet, and email within the Academy provided by ICT staff.
11. I agree that home Internet access is permitted at the discretion of the Principal. I understand the Academy will not accept responsibility for offering technical support relating to home Internet connectivity.
12. I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than Academy premises are not chargeable to the Academy.
13. The ICT support department cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
14. I agree to adhere to Academy policies regarding the following, updated as necessary:

Staff Name	
Date	
Laptop Make/Model:	
Laptop Serial #:	
Laptop Accession #:	
Laptop Name:	
Laptop has Battery:	Yes / No
Laptop has Power lead:	Yes / No
Able to connect to printer:	Yes / No
Able to connect to shared files:	Yes / No
Able to connect to the internet:	Yes / No
Able to connect to the Wireless Network:	Yes / No
Able to connect to Emails:	Yes / No
Able to see Documents	Yes / No
Able to see the Office Templates:	Yes / No
Loan Authorised by Technician Name:	
Technician's signature:	
I have read and agree to be bound by the terms and conditions set out above.	
Staff name:	
Staff signature:	

Any theft should be immediately reported to the police and a crime reference number should be obtained and provided to ICT staff.

Chelsea Academy reserves the right to hold the user financially liable if, through negligence or deliberate action, resources are compromised in any way by them or someone using their user area.