LIFE Education Trust

Learning Is For Everyone

Our Aim is that every School will be:

- An efficient School
- An effective School
- An enriching School
- An enabling School

ICT Policy

Policy	ICT Policy
Policy adopted by Trust Board	25/5/17
Reported to LGBs for implementation	7/6/17
Implementation Date	7/6/17
Review Date	June 2020
Policy Source	Own Sourced Policy

KEY DEFINITIONS USED IN THIS POLICY:

The Trust	LIFE Education Trust
The Board/Directors/Trust Board	The Board of Directors of LIFE Education Trust
School /Trust School	An Academy or School within LIFE Education Trust
Staff	All staff employed by LIFE Education Trust and working with academies, School s or units within LIFE Education Trust

All Schools within the LIFE Education Trust are legally defined as academies, regardless of whether the term “School” is used to describe them in the following policy.

References in this policy to Trust information and systems; ICT equipment etc. includes information, systems and ICT equipment within the Trust Schools.

Each School will designate a member of staff to be the Systems Administrator/ Network manager for the school site. An E-safety officer will also be designated within each School.

Each School will maintain protocols and procedures relevant to specific ICT systems used within the School.

Data Security Policy

SUMMARY

- Ensure the protection of confidentiality, integrity and availability of Trust information and assets.
- Ensure all users are aware of and comply fully with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Definitions

Information - covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers or computers or held in a 'relevant filing system'. This includes paper filing systems.

Strong Password – Password which is 8 characters minimum length, contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, or personal information.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key, on computer systems this is achieved with encryption software.

Responsibilities:

- The Trust shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act.
- Users of the Trust's ICT systems and data must comply with the requirements of the ICT Security Policy.
- The Trust shall review this document at least annually.
- Users shall be responsible for notifying the Network Manager, Headteacher and Trust Data Protection Officer of any suspected or actual breach of ICT security.
- ***The Headteacher shall inform the ICO if there are any losses of personal data*** Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites including the London MLE unless these documents are encrypted.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- Server rooms must be kept locked when unattended and access restricted.

- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- All Trust owned ICT equipment and software should be recorded and an asset register maintained.
- Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security:

- Users shall not make, distribute or use unlicensed software or data.
- Users must ensure they have authorisation for private use of the Trust's computer facilities.
- A Password shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- Each School within the Trust should ensure current and up to date anti-virus software is applied to all ICT systems.
- Laptop users shall ensure they update their virus protection is set to auto update when they are logged on.
- Any suspected or actual virus infection must be reported immediately to the Network Manager/ICT Co-ordinator and that computer shall not be reconnected to the School's network until the infection is removed.

Disposal of Equipment:

- Each School within the Trust shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data. This requires professional software.
- It is important to ensure that any software remaining on a PC being relinquished for reuse is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- Each School within the Trust shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Online Safety Policy: Managing Internet Use

All Schools within the Trust will:

- Maintain broadband connectivity through the LGfL and so connects to the National Education Network;
- Work in partnership with the LA to ensure any concerns about the system are communicated to LGfL so that systems remain robust and protect students;
- Ensure network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc.;
- Ensure their network is 'healthy' by having the Network Manager and LGfL health checks regularly on the network;
- Ensure the Systems Administrator / Network Manager is up-to-date with LGfL services and policies;
- Ensures the Systems Administrator / Network Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows students access to Internet logs;
- Has network auditing software installed;
- Use security time-outs on Internet access where practicable / useful;
- Use individual log-ins for students and all other users, except for Year R;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Use 'safer' search engines with students such as Google and activates 'safe' search where appropriate;
- Ensure students only publish within appropriately secure learning environments. See appendix 1a

Online Safety Policy: Teaching and Learning

All Schools within the Trust will:

- Supervise students' use at all times, and is vigilant in learning resource areas where older students have more flexible access;
- Use the pan-London LGfL / Atomwide filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Plan the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required;
- Use Google for raw image search as set to safe search;
- Inform users that Internet use is monitored;
- Inform staff and students that that they must report any failure of the filtering systems directly to the person responsible for URL filtering. Our systems administrators report to LGfL where necessary;
- Block all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only use approved areas for students' own online creative areas. See appendix 1a
- Only use approved sites for video conferencing such as 'Skype' or 'Go To Meeting'. If in doubt please see the Network Manager
- Only use Moodle, WordPress, G-Suite or school website for blogging – Logins for accounts must be given to CSD so they can access blogs
- Only use approved or checked webcam sites;
- Block student access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;
- Require students and their parent/carer, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Require all staff to sign an Online Safety/ acceptable use agreement form and keeps a copy on file;
- Make 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;
- Keep a record, e.g. print-out, of any bullying or inappropriate behaviour for as long as is reasonable inline with the School behaviour management system;
- Ensure parents/carers provide consent for students to use the Internet, as well as other ICT technologies, as part of the Online Safety acceptable use agreement form at time of their child's entry to the School ;
- Make information on reporting offensive materials, abuse / bullying etc available for pupils, staff and parents;
- Immediately refers any material we suspect is illegal to the appropriate authorities – LA / Police. In accordance with Keeping Children Safe in Education 2016.

Online Safety Policy: Education

All Schools within the Trust will:

- Foster a 'No Blame' environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensure students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or System Manager.
- Ensure students and staff know what to do if there is a cyber-bullying incident;
- Have a clear, progressive Online Safety education programme throughout all Key Stages, built on LA / London / national guidance. Students are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - to STOP and THINK before they CLICK
    - to expect a wider range of content, both in level and in audience, than is found in the School library or on TV;
    - to discriminate between fact, fiction and opinion;
    - to develop a range of strategies to validate and verify information before accepting its accuracy;
    - to skim and scan information;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know some search engines / web sites that are more likely to bring effective results;
    - to know how to narrow down or refine a search;
    - to understand how search engines work;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand 'Netiquette' behaviour when using an online environment such as a 'chat' / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
    - to not download any files – such as music files - without permission;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos;
    - to have strategies for dealing with receipt of inappropriate materials.

- Ensure that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Make training available to staff on Online Safety as appropriate. In depth training at least once per year. Plus Online Safety updates throughout the year;
- Provide advice, guidance and training for parents/carers as necessary.

Online Safety Policy: Infringements and sanctions – Students/Pupils

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile devices in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Sanction - referred to the School's Online Safety Co-ordinator and/or Headteacher]

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile devices after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Sanction - referred to the School's Online Safety Co-ordinator and/or Headteacher]

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending or posting a message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

[Sanction - referred to the School's Online Safety Co-ordinator and Headteacher]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA / Atomwide as appropriate

Category D infringements

- Continued sending or posting messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the School name into disrepute

[Sanction - referred to the School's Online Safety Co-ordinator and Headteacher]

Other safeguarding actions:

1. Secure and preserve any evidence.
2. Inform the sender's service provider.

Online Safety Policy:
Infringements - Employee

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- Unauthorised accessing the Main Network / Email / Internet / Intranet by using someone else's account.

[Referred to the School's Online Safety Co-ordinator and/or Headteacher for sanction]

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any School computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, violent or prejudicial;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the School name into disrepute.

[Referred to the School's Online Safety Co-ordinator and Headteacher for sanction]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop and further access to the School 's network will be blocked.
- Instigate an audit of all ICT equipment by an outside agency, such as the School s ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the School .
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that, the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Each School within the Trust is likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Trust HR provider.

Illegal Material suspected

If illegal material is found or suspected, immediately notify the headteacher. Investigations should never be carried out alone.

- For illegal activity – report to the police
- Illegal content – report to IWF and/or police
- Young person at risk – report to CEOP and police

The Headteacher will immediately consider suspension of staff implicated.

Police contact: free phone number **0808 100 00 40** or http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the School 's Online Safety/ Acceptable Use Policy. All staff will be required to sign the School 's Online Safety Policy acceptance 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 e-safety / acceptable use form;
- The Trust's Online Safety policy will be made available and explained to parents, and parents will sign an acceptance form when their student starts at the School .
- Information on reporting abuse / bullying etc will be made available by the School for students, staff and parents.

Online safety Policy: Use of digital images

All Schools within the Trust will ensure:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to an administration officer.
- The School web site complies with the Trust's guidelines for publications;
- Most material is the School ’s own work; where other’s work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the School address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached. This includes all media posted to social media sites
- They gain parental / carer permission for use of digital photographs or video involving their child as part of the School agreement form when their child joins the School ;
- Digital images /video of students are stored in the teachers’ shared images folder on the network and images are deleted at the end of the year, unless an item is specifically kept for a key School publication;
- They do not use students’ full names when saving images in the file names or in the <ALT> tags when publishing to the School website;
- They do not include the full names of students in the credits of any published School produced video materials / DVDs;
- Staff sign the Trust’s Acceptable Use Policy and this includes a clause on the use of any photographic equipment for taking pictures of students;
- Students are only able to publish to their own ‘safe’ web-portal on approved sites. See appendix 1a
- Students are taught to publish for a wide range of audiences which might include local governors, parents or younger children as part of their ICT scheme of work;
- Students are taught about how images can be abused in their Online education programme.

E-safety Policy: Managing email

All Schools within the Trust will ensure:

- They do not publish personal e-mail addresses of students or staff on the School website. We use anonymous or group e-mail addresses, for example info@School name.la.sch.uk / head@School name.la.sch.uk / info.sch.la@lgfl.net / year3.sch.la@lgfl.net for any communication with the wider public.
- If one of the Trust's staff or students receives an e-mail that is considered to be particularly disturbing or breaks the law, the police will be contacted.
- Accounts are managed effectively, with up to date account details of users.

Students:

- They only use LgfL 'safemail' for students or controlled G-Suite email
- Students should use the School domain e-mail accounts on the School system.
- Students are introduced to, and use e-mail as part of the ~~ICT~~ Computing scheme of work.
- Students are taught about the safety and 'netiquette' of using e-mail i.e.
    - not to give out their e-mail address unless it is part of a School managed project or 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, short and concise;
    - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on School headed paper;
    - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;
    - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
    - the sending of attachments should be limited;
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher / responsible adult if they receive an e-mail 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 e-mails, but to keep them as evidence of bullying;
    - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
    - that forwarding 'chain' e-mail letters is not permitted;

- Students sign the Trust Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff should use School e-mail systems for professional purposes; including cover work to ensure prompt delivery.
- Access in School to external personal e-mail accounts may be blocked;
- Staff are aware that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on School headed paper. That it should follow the School 'house-style';
    - the sending of attachments should be limited;
    - the sending of chain letters is not permitted;

- embedding adverts is not allowed;

- Staff sign the appropriate Trust's Agreement Form to say they have read and understood the Online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Online safety Policy: Online Bullying and Child Protection

"Bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form."

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of School time.

1. Advise the child not to respond to the message
2. Refer to relevant policies including Online Safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
3. Secure and preserve any evidence – Get screenshots if the bullying has taken place on a mobile device. If you are unsure how to do this please consult with Network Manager.
4. Inform the sender's e-mail service provider
5. Notify parents/carers of the children involved
6. Consider delivering a parent workshop for the School community
7. Consider informing the police depending on the severity or repetitious nature of offence
8. Inform the LA Online Safety officer

If malicious or threatening comments are posted on an Internet site about a pupil or member of staff:

1. Inform and request the comments be removed if the site is administered externally
2. Secure and preserve any evidence
3. Send all the evidence to the Head of Harm Reduction at CEOP at ww.ceop.gov.uk/contact_us.html
4. Endeavour to trace the origin and inform police as appropriate
5. Inform LA Online Safety officer

"As with all forms of harm or abuse, there is no exhaustive list of signs or indicators to watch out for. But these can include: changes in children's behaviour, demeanour, physical appearance and presentation, language or progress. "

If you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child:

1. Report to and discuss with the named Designated Safeguarding Lead in School and contact parents
2. Advise the child on how to terminate the communication and save all evidence
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services
5. Inform Online Safety officer

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Handling a sexting /naked selfie incident:

There should always be an initial review meeting, led by the Designated Safeguarding Lead (DSL) School . This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people, when assessing the risks the following should be considered:
    - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
    - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
    - Are there any adults involved in the sharing of imagery?
    - What is the impact on the pupils involved?
    - Do the pupils involved have additional vulnerabilities?
    - Does the young person understand consent?
    - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another School , college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents or carers should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply then a School may decide to respond to the incident without involving the police or children's social care (a School can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the School 's pastoral support and disciplinary framework and if appropriate local network of support.

ICT ACCEPTABLE USE POLICY : Agreement Form for Trust Employees, Volunteers and Governors

Covers use of all digital technologies in School :

EMAIL / INTERNET / INTRANET / NETWORK RESOURCES / LEARNING PLATFORM / SOFTWARE / EQUIPMENT / SYSTEMS / iPADS / CHROMEBOOKS /*LAPTOP* POLICY

- I understand that it is a criminal offence to use a Trust ICT system for a purpose not permitted by its owner.

- I will only use the School 's Communication Software Hardware for Professional purposes or for uses deemed 'reasonable' by the Head and Local Governing Body.

- I appreciate that ICT includes a wide range of systems, including but not limited to mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for School business.

- I will only use the approved secure email system(s) for any Academy business. I am a representative of LIFE Education Trust and when I am on the Internet and/or using email:

    - I will make sure that my actions are in the interest (and spirit) of the Trust and I will not leave the Trust open to legal action (e.g. libel).
    - I will avoid trading insults with other people using the Internet with whom I disagree.
    - Any e-mail sent to an external organisation will be written carefully before sending, in the same way as a letter written on School headed paper.
    - I will not browse, write, bookmark, access or download anything that may be considered offensive to colleagues or the Trust.
    - I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
    - I will not forward emails warning about viruses (they are invariably hoaxes and the Network Manager will probably already be aware of genuine viruses - if in doubt, contact them for advice).
    - I will not open emails unless I have a reasonably good expectation of what it contains (e.g. do open report.doc from an Internet colleague I know (But check before opening if you were not expecting the attachment, it has a long link or something just looks wrong. (Be careful Ransomware can come from an email contact who you know). Do not open explore.zip sent from an address I've never heard of, however tempting. I will alert the Network Manager if I am sent anything like this unsolicited).
    - (See Appendix A – Email Protocol and Appendix B – Good Practice Guide)

- I will not attempt to gain unauthorised access to information or facilities that are outside of my professional role. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. If I do not have access to information resources that I feel I need then I will contact my line manager.

- I will ensure that I do not disclose personal system passwords or other security details to other staff, students, volunteers or external agents without proper authorisation and I will not use anyone else's login as this compromises the security of the School . If someone else gets to know my password, I will ensure that I change it or contact the Network Manager for assistance.

- I will not allow unauthorised individuals to access Email / Internet / Intranet or other School / LA systems using my account.

- If I leave a PC, laptop or tablet unattended without logging off, I am responsible for any misuse of it while I am away.

- I understand that, if any PC in a public area where other staff users have the right to use that PC (e.g. staffroom) is found to be locked by a user while they are away the Network Manager reserves the right to unlock that PC for anyone else to use, potentially losing any unsaved work.

- I will ensure that any printed communication with parents, students and public bodies will be approved by the Headteacher.

- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager.

- I will ensure all documents are saved, accessed and deleted in accordance with the School 's network security and confidentiality protocols.

- I will ensure that important data is sufficiently backed up, particularly with regard *to any loaned ICT equipment such as a laptop.* Preferably, data will be backed up in more than one place to prevent total loss by e.g. losing a USB drive or the laptop breaking down, while still ensuring that the data is safe and in accordance with basic security and confidentiality protocols.

- I will not connect a computer or laptop to the network / Internet unless authorised by the Network Manager/Computing Coordinator

- I will make best efforts to ensure that I do not store large quantities of data in my personal account area, especially if it is materials which can benefit other members of staff for their lessons – e.g. video clips. I will save these to the departmental shared area.

- I will not connect a School laptop or other device that belongs to the School to a network / Internet other than at home or at School unless authorised to do so.

- I will not use digital cameras or camera phones for transferring images of pupils or colleagues without permission.

- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.

- I will only access the School 's networks / email / Internet / Intranet using my own authorised account and will not use anyone else's account.

- I will not connect a computer, laptop or other device to the network / Internet that does not have up-to-date anti-virus software.

- I will make best efforts to ensure any USB drives or other storage devices that I connect to a School PC or any loaned ICT equipment will not compromise the School network. I will always scan and check the USB upon installation and any information that is sensitive or includes names will be encrypted and deleted as soon as it is no longer needed.

- I will keep any 'loaned' ICT equipment such as a laptop or other ICT device up-to-date, using the School 's recommended system and make best efforts to ensure that the anti-virus and other anti-malware-related software is kept up-to-date and that I run regular scans on

the equipment during the time I loan the equipment. the Network Manager should be notified if assistance is required.

- I will use the School 's Learning Platform in accordance with Trust / and LGfLadvice.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow Trust data security protocols when using any such data at any location.
- I will not support or promote extemist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the School 's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that all Internet and email usage will be logged and this information could be made available to my manager on request.
- I will not try to resolve any issues regarding the use of ICT facilities unless I have been authorised to do so. I will raise any issues that may occur to the Network Manager/Computing Coordinator via my line manager or using the IT helpdesk. I will not permit any students to try to fix any issues with the ICT facilities unless they are authorized to do so.
- I understand that all Internet usage will be logged on the laptop and I will not try tofalsify this information. This information could be made available to my manager on request. Any issues regarding Internet usage should be raised with the line manager, senior management or to the Network Manager.
- I understand that I am responsible for the use of the ICT equipment on loan and I will not allow any unauthorised use of the equipment by friends or family.
- I will ensure that any private social networking sites/blogs etc. that I create or actively contribute to are not confused with my professional role and I will make best efforts to ensure that any such contributions I make will not bring the School or other staff into disrepute.
- I will not engage in online activity that may compromise my professional role. See Appendix C – Social Networking.
- I agree and accept that any computer or laptop loaned to me by the School , is provided solely to support my professional responsibilities and that I will notify the School of any "significant personal use" as defined by HM Revenue & Customs.
- I will only use Local Authority systems in accordance with any Corporate policies.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.
- I will return my 'on loan' laptop or other ICT device belonging to the School when leaving the School to the Headteacher or their nominated representative.

- I understand that it is my duty to support the whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be innappropriate or concerning in any way, to a senior member of staff or the designated Child Protection Lead.

- I understand that Internetencrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

Appendix A Email Protocol –Code of Conduct

Users must:

- within working hours, respond to emails in a timely and appropriate fashion. The system is designed for speedy communication. If urgent, the email requires a prompt response, otherwise a response should be sent within a reasonable timeframe according to the nature of the enquiry;
- not use anonymous mailing services to conceal identity when mailing through the Internet, falsify e-mails to make them appear to originate from someone else, or provide false information to any Internet service which requests name, e-mail address or other details;
- not abuse others (known as 'flaming'), even in response to abuse directed at themselves;
- not use electronic media and services in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system;
- not use, transfer or tamper with other people's accounts and files;
- not use their own equipment to connect to the School's network unless specifically permitted to do so and the equipment meets appropriate security and other standards. Not under any circumstances use personal equipment containing inappropriate images or links to them, to be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work in a School or with children.
- ensure that pupils are not exposed to any inappropriate images or web links whether on School owned computers or on their own computer/equipment used for School purposes (where this has been authorised). School/service and adults need to ensure that internet equipment used by children have the appropriate controls with regards to access. E.g. personal passwords should be kept confidential.;
- not store sensitive or confidential data on their own equipment – this extends to personal cameras, mobile phones and other similar devices;
- use unsecured disks/memory sticks (all disks/memory sticks used must be encrypted and/or password protected);
- respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner;
- not use the internet/intranet facilities or equipment to deliberately propagate any virus, worm, Trojan horse or any such other programme that is harmful to normal computer operations;

If a user finds they are connected accidentally to a site that contains sexually explicit or offensive material, they must disconnect from that site immediately. Such unintentional access to inappropriate internet sites must be reported immediately to their line manager. Any failure to report such access may result in disciplinary action.

Except in cases in which explicit authorisation has been granted by an appropriate manager, employees are prohibited from engaging in, or attempting to engage in:

- monitoring or intercepting the files or electronic communications of other employees or third parties;
- hacking or obtaining access to systems or accounts they are not authorised to use;
- using other people's log-ins or passwords;
- breaching, testing, or monitoring computer or network security measures;
- interfering with other people's work or computing facilities;
- sending mass e-mails without consultation with the Head teacher. Global sends (send to everybody in the Global address book) are prohibited;

Appendix B Email Good Practice Guide –Code of Conduct

Good Practice	
Read receipt	When it is important to know that a recipient has opened a message, it is recommended that the sender invoke the 'read receipt' option.
Attachment formats	When attaching a file it will have a specific format. Be aware of the possibility that a recipient may not have the software necessary to read the attachment. Format incompatibility can occur even between successive versions of the same software, e.g. different version of Microsoft Word.
E-mail address groups	If messages are regularly sent to the same group of people, the addressing process can be speeded up by the creation of a personal group in the personal address book.
Message header, or subject	Convey as much information as possible within the size limitation. This will help those who get a lot of e-mails to decide which are most important, or to spot one they are waiting for.
Subject	Avoid sending messages dealing with more than one subject. These are difficult to give a meaningful subject heading to, difficult for the recipient to forward on to others for action, and difficult to archive.
Recipients	Beware of sending messages to too many recipients at once. When sending messages for more than one-person's use be sure to indicate people for whom there is some expectation of action or who have central interest. cc to indicate those who have peripheral interest and who are not expected to take action or respond unless they wish to do so.
Replying	When replying to a message sent to more than one person, do not routinely reply to all recipients of the original message. Consider who needs to read your reply, e.g. if the sender is organising a meeting and asking you for availability dates, you need only reply to the sender.
Absent	If you have your own e-mail address, it is possible, for users of MS Exchange or have local enhancements to MS-mail, to set the 'out of office' message when you are going to be away for some time, e.g. on annual leave. You won't lose your messages, they will await your return, but the sender will know that you're not there and can take alternative action if necessary.
Evidential record	Never forget that electronic conversations can produce an evidential record which is absent in a telephone conversation. Comments made by an employee during the course of an exchange of e-mails could be used in support, or in defence, of the school's legal position in the event of a dispute.
Legal records	Computer generated information can now be used in evidence in the courts. Conversations conducted over the e-mail can result in legally binding contracts being put into place.
Distribution lists	Keep personal distribution lists up-to-date and ensure you remove individuals from lists that no longer apply to them
E-Mail threads	Include the previous message when making a reply. This is called a thread. Threads are a series of responses to an original message. It is best that a response to a message is continued by using reply accessed on the quick menu bar, rather than start an entirely new message for a response. Keep the thread information together. It is easier for the participants to follow the chain of information already exchanged. If the message gets too long the previous parts can be edited while still leaving the essence of the message.
Context	E-mail in the right context, care should be taken to use e-mail where appropriate. There may be occasions when a telephone call would be more appropriate especially on delicate matters. Beware of the use of excessive use of capitals. It can be interpreted as shouting so consider how the style of your email may be interpreted by its recipient.
Forwarding e-mails	Consideration should be given when forwarding e-mails that it may contain information that you should consult with the originator before passing to someone else.
Large e-mails	For larger e-mails, particularly Internet e-mails, where possible send at the end of the day as they may cause queues to form and slow other peoples e-mail.

Appendix C Social networking – Code of Conduct

Access to Social Networking Sites

Staff should adhere to the policy and procedures regarding the ICT usage including Social Networking Sites as set out in the ICT Policy. All employees should understand the implications of inappropriate and improper use of social networking sites at home in their own personal time that may result in disciplinary action being taken.

The following permissions are given in respect of social networking applications:

a) Complete block from personal use during working time and/or using the school's computer network.

Managing social networking sites

This may include internal forums for staff and outward facing forums for School activities/clubs etc.

It is important to ensure that employees, members of the public and other users of online services know when a social networking application is being used for official school/ purposes. To assist with this, all employees must adhere to the following requirements:

- only use an official (i.e. not personal) email addresses for user accounts which will be used for official purposes;
- appropriate feedback and complaints information must be published in a prominent place which is easily accessible to other users;
- the school's logo and other branding elements should be used where appropriate to indicate the school's support. The school's logo should not be used on social networking applications which are unrelated to or are not representative of the school's official position;
- employees should identify themselves as their official position held within the School on social networking applications. eg through providing additional information on user profiles;
- employees should ensure that any contributions on any social networking application they make are professional and uphold the reputation of the school– the general rules on internet/email apply;
- employees should not spend an unreasonable or disproportionate amount of time during the working day developing, maintaining or using sites;
- employees must not promote or comment on personal matters (including personal/ financial matters), commercial ventures, political matters or campaigns, religious or other matters;
- employees should be aware that sites will be monitored.

Personal social networking sites

All employees of the school, individuals engaged by the School or individuals acting on behalf of the School from third party organisations should bear in mind that information they share through social networking applications, even if they are on private spaces, may still be the subject of actions for breach of contract, breach of copyright, defamation, breach of data protection, breach of confidentiality, intellectual property rights and other claims for damages. Employees must therefore not publish any content on such sites that is inappropriate or may lead to a claim, including but not limited to material of an illegal, sexual or offensive nature that may bring the School or the local authority into disrepute (see Appendix B for examples of such content).

Employees using social networking sites must also operate at all times in line with the school's Equality and Diversity policy, failure to do so may lead to disciplinary action, up to and including dismissal.

Social networking applications include, but are not limited to, public facing applications such as open discussion forums and internally-facing applications, (i.e. e-folio) regardless of whether they are hosted on School networks or not. The School expects that users of social networking applications will always exercise due consideration for the rights of others and that users will act strictly in accordance with the terms of use set out in this code.

Any communications or content published on a social networking site which is open to public view, may be seen by members of the School community. Employees hold positions of responsibility and are viewed as such in the public domain. Inappropriate usage of social networking sites by employees can have a major impact on the employment relationship. Any posting that causes damage to the school, any of its employees or any third party's reputation may amount to misconduct or gross misconduct which could result in disciplinary action, up to and including dismissal. Employees must not use social networking sites for actions that would put other employees in breach of this policy.

Employees should not use personal sites for any professional activity or in an abusive or malicious manner. The School reserves the right to require the closure of any applications or removal of content published by employees which may adversely affect the reputation of the School or put it at risk of legal action.

Posting inappropriate images

Indecent images of any employee that can be accessed by students, parents or members of the public are totally unacceptable and can lead to child protection issues as well as bringing the School into disrepute.

Posting inappropriate comments

It is totally unacceptable for any employee to discuss pupils, parents, work colleagues or any other member of the School community on any type of social networking site.
Reports about oneself may also impact on the employment relationship for example if an employee is off sick but makes comments on a site to the contrary.

Social interaction with pupils (past and present)

Employees should not engage in conversation with pupils on any personal social networking sites and should be circumspect in personal network contact with former pupils, particularly those under the age of 18 years. This would also apply to individuals who are known to be vulnerable adults. Offers of assistance to a pupil with their studies via any social networking site are inappropriate and also leaves the employee vulnerable to allegations being made. It would be very rare for employees to need to interact with pupils outside of School in a social setting and by communicating with them on social networking sites, is tantamount to the same. Individuals working in the School should ensure that personal social networking sites are set at private and that pupils are never listed as approved contacts.

Individuals working in the School should not use or access social networking sites of pupils.

Making Friends

Employees should be cautious when accepting new people as friends on a social networking site where they are not entirely sure who they are communicating with. Again this may leave employees vulnerable to allegations being made.

Covers use of digital technologies in School :

EMAIL / INTERNET / INTRANET / NETWORK RESOURCES / LEARNING PLATFORM / SOFTWARE / EQUIPMENT / SYSTEMS / iPADS / CHROMEBOOKS *LAPTOP* POLICY

Employee/Volunteer/Governor COPY

User Signature

I have read and been provided with a copy of the above mentioned Policy.
I agree to abide by the terms and conditions of the Acceptable Use Policy.
I understand that I have responsibility for my own and others online safeguarding and I undertake to be a 'safe and responsible user.'

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

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

Signature …… Date …….

Full Name ……..(printed)

Job title . . . . . .

Authorised Signature (Head Teacher)

Is this member of staff temporary? NO / YES

If yes, contract end date: …….

I approve this email account / connection to the Internet / Intranet.

Signature …….... Date …….

Full Name ……..….(printed)

Covers use of digital technologies in School :

EMAIL / INTERNET / INTRANET / NETWORK RESOURCES / LEARNING PLATFORM / SOFTWARE / EQUIPMENT / SYSTEMS / iPADS / CHROMEBOOKS *LAPTOP* POLICY

SCHOOL COPY

User Signature
I have read and been provided with a copy of the above mentioned Policy.
I agree to abide by the terms and conditions of the Acceptable Use Policy.
I understand that I have responsibility for my own and others online safeguarding and I undertake to be a 'safe and responsible user.'

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

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

Signature …… Date …….

Full Name ……..(printed)

Job title . . . . . .

Authorised Signature (Head Teacher)

Is this member of staff temporary? NO / YES

If yes, contract end date: ……

I approve this email account / connection to the Internet / Intranet.

Signature …….... Date …….

Full Name ……..….(printed)

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

KEEPING SAFE: STOP, THINK, BEFORE YOU CLICK!

- I will keep my login and password secret.
- I will not bring files into School without permission or upload inappropriate material to my workspace.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the School. I am aware that some websites and apps including social networks and games have age restrictions and I should respect them.
- I will only e-mail people I know, or who my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible. I will not participate in any form of Online bullying.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent or guardian has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

LIFE Education Trust

Use of digital images - photography and video

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

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

If the student is named, we avoid using their photograph.
If their photograph is used, we avoid naming the student.

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

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

Only images of students in suitable dress are used.
Staff are not allowed to take photographs or videos on their personal equipment.

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

- Your daughter / son being photographed (by the classroom teacher, teaching assistant or another student) as part of a learning activity,e.g. photographing students at work and then sharing the pictures on the Interactive whiteboard in the classroom allowing the students to see their work and make improvements.
- Your daughter's/son's image for presentation purposes around the School; e.g. in School wall displays and PowerPoint© presentations to capture images around the School or in the local area as part of a project or lesson.
- Benhurst Primary School also work closely with SMART Technologies who regularly visit the school and take photographs and short videos for advertising, publicity and commercial purposes.

Your daughter's/son's image being used in a presentation about the School and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, School s or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our School prospectus or on our School website. In rare events, your daughter/son could appear in the media if a newspaper photographer or television film crew attend an event.

Note: If we, or you, actually wanted your daughter's/son's image linked to their name we would contact you separately for permission, e.g. if your daughter/son won a national competition and wanted to be named in local or government literature.
Further information for parents on Online safety can be found at: http://www.parentscentre.gov.uk/usingcomputersandtheinternet/linksbytopic/

LIFE Education Trust

Online Safety agreement form: parents/carers

Parent / Carer name: _____

Student's name: _____

As the parent or legal guardian of the above pupil, I grant permission for my daughter / son to have access to use the Internet, e-mail and other ICT facilities at School.

I know that my daughter / son has signed an Online safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the School will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching Online safety skills to students.

I understand that the School can check my daughter's /son's computer files, and the Internet sites they visit, and that if they have concerns about their Online safety or Online behaviour that they will contact me.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my daughter's / son's Online safety.

Parent / Carer signature: _____ **Date:** ___/___/___

Use of digital images - photography and video: I also agree to the School using photographs of my daughter / son or including them in video material, as described in the document 'Use of digital images - photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the School, and for no other purpose.

I understand that the school has a clear policy on "The use of social networking and media sites," and I support this.

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

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

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

Parent / Carer signature: _____ **Date:** ___/___/___

School Copy

Online Safety agreement form: parents/carers

Parent / Carer name: _____

Student's name: _____

As the parent or legal guardian of the above pupil, I grant permission for my daughter / son to have access to use the Internet, e-mail and other ICT facilities at School.

I know that my daughter / son has signed an Online safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the School will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access e-mail, employing appropriate teaching practice and teaching Online safety skills to students.

I understand that the School can check my daughter's /son's computer files, and the Internet sites they visit, and that if they have concerns about their Online safety or Online behaviour that they will contact me.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my daughter's / son's Online safety.

Parent / Carer signature: _____ **Date:** ___/___/___

Use of digital images - photography and video: I also agree to the School using photographs of my daughter / son or including them in video material, as described in the document 'Use of digital images - photography and video'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the School , and for no other purpose.

I understand that the school has a clear policy on "The use of social networking and media sites," and I support this.

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

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

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

Parent / Carer signature: _____ **Date:** ___/___/___ **Parent Copy**

Online Safety agreement form: Student

KEEPING SAFE: STOP, THINK, BEFORE YOU CLICK!

Student name: _____

Form:_____

I have read or have had read to me the School 'rules for responsible ICT use'.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and all ICT software and devices in a safe and responsible way. I understand that the School can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / guardian.

Student's signature _____

Date: ___/___/___

Student Copy

Online Safety agreement form: Student

KEEPING SAFE: STOP, THINK, BEFORE YOU CLICK!

Student name: _____

Form:_____

I have read or have had read to me the School 'rules for responsible ICT use'.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and all ICT software and devices in a safe and responsible way. I understand that the School can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / guardian.

Student's signature _____

Date: ___/___/___

School Copy

Twitter Policy

- Make sure the account remains locked (Protect my tweets)
- Secure the account (require personal information to reset password)
- Use a very secure password that is different form your School user account (this will be set by the Network Manager)
- Be careful who you follow
- Be careful re-tweeting other messages
- You must be registered with your work E-mail address
- Do not add locations to your tweets
- We advise switching off Email updates for most settings as you will get lots of E-mails coming through
- We will use the name of the Academy for departmental accounts. For teachers' accounts we will use your first initial and then surname. Eg. J.Bloggs
- Please use the same theme to the Twitter account as the main School theme.

When Posting

- Don't post personal details
- Consider your posts, are they useful or informative
- Only post appropriate material
- Do not post any kind of derogatory comments
- Be professional – try to avoid text speak e.g. lol, m8, etc.
- Try not to post to often as people will not want get constantly spammed by your account
- If you receive offensive tweets please block the user and report it to the network manager

Consider who you follow and what they might post, or what their website might link to. A general rule is if you can get to inappropriate material in less than five clicks then do not follow them.

Account type

Twitter only offers one type of account but at FBA we have decided to categorize three account types you can use:

Personal Account – This is your own personal account used outside of work. Do not give out details of this account to any students and do not follow any students.

Department Account – must be made private - This can be used by departments to broadcast messages to students. Any student can follow but do not follow students.

School Account – public account – This will be used by the School and can be followed by students, parents, teachers, etc. We will not follow students, only people or groups that have a connection with the School .

(Please note these are not actual settings on twitter if you need more info please consult the Network Manager)

BYOD (Bring Your Own Devices) Policy

We are happy for people to bring in their own devices to use on the network but you must adhere to the following rules.

Staff

- Staff must bring their devices to the IT department so that we can connect them to the staff wireless network.
- Staff will need to sign in once every 30 days using their USO account.
- We do not give out the passkey to anyone for this network. It should only be known by members of the IT team. If this key is made public we will be required to change it.
- Any laptops that connect to the network should have up to date antivirus.
- Devices should also have passwords in place and devices should lock themselves automatically if not used for more than 5 minutes.
- Staff are responsible for the security and safety of their own devices that they bring into School .
- The Network Manager will support the device as far as getting it connected to the network. The Network Manager will not be responsible for fixing issues on staff personal devices.
- All existing ICT policies still apply when using personal devices.

Student

- Students can connect to the student wireless network using the passkey that is displayed around the School .
- They will need to sign in using their USO account once a week.
- Any laptops that connect to the network should have up to date antivirus.
- Devices should also have passwords in place and devices should lock themselves automatically if not used for more than five minutes.
- Students are responsible for the security and safety of their own devices that they bring into School .
- The Network Manager will support the device as far as getting it connected to the network. The Network Manager will not be responsible for fixing issues on students personal devices.
- All existing ICT policies still apply when using personal devices.
- Students should not use their cameras whilst in School to take selfies or photos of other students or staff without permission.
- If students do take photos they must not be published anywhere including social media sites.
- Students should only use apps that their teachers tell them to use for School work. No other apps should be used during lesson.
- We do not allow the use of live streaming at any time. Apps such as Periscope, Facebook Live, Twitter Live, Twitch, etc. are all banned.

Guests

- Guests can connect to the guest network. The passkey is available from the school's designated staff members.
- Guests will be required to sign a copy of the Visitors Acceptable Use Policy.
- Guests will be required to read and acknowledge a set of rules before connecting (This page automatically displays once they connect to the network)
- Any laptops that connect to the network should have up to date antivirus.
- Devices should also have passwords in place and devices should lock themselves automatically if not used for more than five minutes.

- Guests are responsible for the security and safety of their own devices that they bring into School.
- The Network Manager will support the device as far as getting it connected to the network. The Network Manager will not be responsible for fixing issues on staff personal devices.
- All existing ICT policies still apply when using personal devices.
- If any visitors wish to use a USB this must be virus checked before use.

Appendix – 1 A

Approve learning platforms and sites

- LGFL Resources – Using USO account
- G-Suite – School issued accounts only
- SMART Amp
- ePortfolio