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 updated in line with General Data Protection Regulations 25/5/18
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.

This policy has been updated in respect of the General Data Protection Regulations effective 25th May 2018

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 6 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 DPO shall inform the ICO if there are any losses of personal or special category personal data*** Users must comply with the requirements of the General Data Protection Regulations, 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.

E-Security Policy

Strategic & Operational Practices

In the Trust:

1. The Headteacher is the Senior Information Risk Officer (SIRO)
2. SDS DPO Services email: sps-dpo-services@isystemsintegration.com is the Data Protection Officer (DPO) with responsibility for data protection compliance
3. Staff are clear who the key contact(s) for key school information are (the Information Asset Owners). This can be located in T Drive/Staff Documents/GDPR
4. We ensure staff know to immediately report, and who to report to, any incidents where data protection may have been compromised, such as when passwords for sensitive systems or devices are lost or stolen, so that relevant action(s) can be taken.
5. All staff are DBS checked and records are held on the Single Central Record and in SIMSs.
   We ensure ALL the following school stakeholders sign an Acceptable Use Agreement.
   We have a system so we know who has signed.
   a. Staff
   b. Governors
   c. Students
   d. Parents
   e. Volunteers
   This makes clear all responsibilities and expectations with regard to data security
6. We have approved educational web filtering across our wired and wireless networks.
   We also have Netsupport DNA monitoring the network.
   We monitor school emails and G-Suite activity to ensure compliance with the Acceptable Use Agreement. As well as monitoring usage, we may also monitor content of emails/work etc.
7. We follow LIFE Education Trust guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services.
8. All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
9. We require staff to use a different password for SIMs than the one they use to access computers.
10. We require that any personal/sensitive material must be encrypted if the material is to be removed from the school, and limit such data removal. Data can only be transferred using encrypted devices or your school G-Suite account
11. School staff who set up usernames and passwords for email, network access, work within the approved system and follow the security processes required by those systems
12. We ask staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical or Manual solutions

1. Staff have Staff Drive on Google Drive to store sensitive documents or photographs
2. We require staff to log-out of systems when leaving their computer
3. We use encrypted flash drives or GoogleSuite if any member of staff has to take any sensitive information off site.
4. All staff are required to sign up to Egress Switch, a secure email and file transfer tool when sending sensitive information off site.
5. We use RAv3 for remote access into our systems
6. We use the DfE S2S site to securely transfer CTF pupil data files to DfE/other schools.
7. We use LGfL AutoUpdate for creation of online user accounts for access to services and online resources
8. We use Google Suite for online document storage

9. We store any sensitive/special category written material in lockable storage cabinets
10. All servers are in lockable locations and managed by DBS checked staff
11. Back ups are encrypted and stored in a locked room or in a secure off site area
12. We comply with the WEEE directive on equipment disposal, by suing an approved disposal company for disposal of IT equipment. For systems, where any protected or restricted data has been held, (such as servers, photocopiers), we get a certificate of secure deletion.
13. Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
14. Paper based sensitive information is shredded using an approved external contractor and a certificate of secure deletion is obtained

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.

Acceptable Use Agreement: Staff, Volunteers, Governors & Contractors

Covers use of all digital technologies while in school: i.e. **email, internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school or school umbrella body (Local Authority, Academy, Free School Trust, etc).**

Also covers school equipment when used outside of school, use of online systems provided by the school or school umbrella body when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.

LIFE Education Trust regularly reviews and updates all AUP documents to ensure that they are consistent with the school Online Safety Policy.

These rules will help to keep everyone safe and to be fair to others. Please note that school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school or school umbrella.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
  This is currently: *LGfL StaffMail*
- I will only use the approved method/s of communicating with pupils or parents/carers: *email system LondonMail*, and only communicate with them in a professional manner and on appropriate school business.
- I will not support or promote extremist 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 will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the appropriate line manager / school named contact *the Network Manager or Data Protection Lead*.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's *recommended anti-virus and other ICT 'defence' systems*.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the school's policy on use of mobile phones / devices at school and will not use them during working hours
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will only I take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, online learning environment etc. will not identify students by name, or other personal information.
- I will use the school's Learning Platform or online cloud storage service in accordance with school protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- 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 access school resources remotely (such as from home) using the *LGfL / school approved system* and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- 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 am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have extended responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected. The school's data protection officer must be aware of all data storage.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the relevant Senior Member of Staff / Designated Safeguarding Lead.

- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head* / *Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- *Staff that have a teaching role only:* I will embed the school's online safety / digital literacy / counter extremism curriculum into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff, Volunteers, Governors

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent online safety / safeguarding policies.

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

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

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

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

Full Name ..... (printed)

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.

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 regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies, on each school's websites. We attempt to ensure that all students have good access to digital technologies to support their teaching and learning and we expect all our students to agree to be responsible users to help keep everyone safe and to be fair to others.

Your child/young person will be asked to read and sign an Acceptable Use Policy tailored to his/her age. Please read this carefully – it is attached below and can be found on the school's websites.

Parents Acceptable Use Agreement

Internet and IT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to:

- the internet at school
- the school's chosen email system
- Google Suite, Office 365 Moodle, SMARTAmp, SMART Learning Suite online, Show My Homework, Doddle and any other online teaching resources we use in school

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 takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

I understand that all internet and device use in school is subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used in the same manner as when in school.

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this.

I understand that the school will necessarily use photographs of my child or including them in video material to support learning activities.

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose.

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. The impact of social media use is often felt in schools, and this is why we expect certain behaviours from pupils when using social media at all times.

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 inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or share any material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.

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.

Name(s) of pupil/student: _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

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

LIFE Education Trust rules for any external use of digital images are:

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

Where showcasing examples of pupils' 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 pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils 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 at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made by a nursery child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays or PowerPoint© presentations.

- Your child'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, schools or educators, e.g. in our school prospectus or on our school website. On rare occasions, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if they won a national competition and wanted to be named in local or government literature.

The use of social networking and online media

This school asks its whole community to promote the 'three commons' approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory, or encourage extremist views. This is online bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. Creating or forwarding such materials can make us liable for prosecution.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any websites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

If any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on the internet or any social media, they will be reported to the appropriate 'report abuse' section of the network site (all social media have clear rules about content which can be posted and have robust mechanisms to report breaches). Pupils and staff would be disciplined appropriately, and we expect parents to support us in this and behave appropriately themselves.

In serious cases, we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP process for reporting inappropriate sexual approaches towards children at thinkuknow.co.uk/parents

Key Stage 1: Acceptable Use Agreement

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep ~~**SECRETS**~~ just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults are _____ at school

_____ at home and _____

My name is _____

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others

- ***I am an online digital learner*** – I use the school's internet and devices for schoolwork, homework and other activities to learn and have fun. I only use sites, games and apps that my trusted adults say I can.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out.
- ***I am careful online*** – I think before I click on links and only download when I know it is safe or has been agreed by trusted adults. I understand that some people might not be who they say they are, so I should be very careful when someone wants to be my friend.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my home address, phone number or other personal information that could be used to identify me or my family and friends.
- ***I keep my body to myself online*** – I never change what I wear in front of a camera and remember that my body is mine and mine only, and I don't send any photos without checking with a trusted adult.
- ***I say no online if I need to*** – if I get asked something that makes me worried or upset or just confused, I say no, stop chatting and tell a trusted adult.

- ***I am a rule-follower online*** – I know that some websites and social networks have age restrictions and I respect this; I only visit sites, gams and apps that my trusted adults have agreed to.
- ***I am considerate online*** – I do not join in with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not post, make or share unkind, hurtful or rude messages/comments and tell my trusted adults if I see these.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed or is worried or upset by things they read, watch or hear.
- ***I don't do public live streams on my own*** – and only go on a video chat if my trusted adult knows I am doing it and who with.
- ***I communicate and collaborate online*** – with people I know and have met in real life or that a trusted adult knows about.
- ***I am SMART online*** – I understand that unless I have met people in real life, I can't be sure who someone is online, so if I want to meet someone for the first time, I must always ask a trusted adult for advice.
- ***I am a creative digital learner online*** – I don't just spend time online to look at things from other people; I get creative to learn and make things! I only edit or delete my own digital work and only use other people's with their permission or where it is copyright free or has a Creative Commons licence.

- ***I am a researcher online*** – I use safer search tools approved by my trusted adults. I understand that not everything online can be believed, but I know how to check things and know to 'double check' information I find online.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: _____ Date: _____

KS3-4 Pupil Online Acceptable Use Agreement

LIFE Education Trust regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies, which can be found on the school's websites.

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

1. I will be a responsible user and stay safe when using the internet and other digital technology at school.
2. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
3. I will only use the school's internet and any device I may be using in school for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or after school.
4. I understand that all internet and device use in school may be subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used as if I am in school.
5. I will keep my logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it.
6. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
7. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
8. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
9. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
10. I understand that cyberbullying is unacceptable, and will not use technology to bully, impersonate, harrass, threaten, make fun of or upset anyone, at school or outside.
11. I will not browse, download, upload, post, retweet or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
12. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions and I should respect this.
13. I will only e-mail or contact people as part of learning activities.
14. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
15. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
16. When using the internet, I will not download copyright-protected material (text, music, video etc.)
17. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

18. Live streaming can be fun but I always check my privacy settings and if I rarely (or preferably never) do anything that everyone on the internet can see. If I live stream, I tell a trusted adult about it.
19. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
20. I will only use my personal devices (mobile phones, USB devices etc) in school if I have been given permission to do so.
21. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
22. I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
23. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
24. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, I will not respond to it but I will save it and talk to a trusted adult.
25. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
26. I know who my trusted adults are at school, home and elsewhere, but if I feel I can't talk to them, I know I can call Childline or click CEOP.

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

Signed: _____ ***Date:***_____

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 in LIFE 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

Approved learning platforms and sites

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