7g. Acceptable Use of ICT Policy

Introduction

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and, if applicable, regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Whilst a major focus of the document lies with access to the Internet and use of email, the document also covers acceptable use of the equipment and resources provided by the school and general behaviour whilst using them.

To provide the correct *context* for this policy, the document starts by outlining the school's attitude towards the educational benefits of ICT, how the school intends to incorporate ICT within the wider curriculum, and how the school intends to promote safe and responsible use of the technology to pupils and staff.

Contents

- Aim of the policy
- Roles and responsibilities
- Online behaviour
- Using the school's IT systems
- Passwords
- Use of Property
- Promoting Safe Use of ICT and the Internet
- Monitoring and Access
- Compliance with Related School Policies
- Acceptable use by parents and carers
- Acceptable use by visitors, contractors and others
- Health and Safety
- Retention of Digital Data
- Breach Reporting
- Security and Software Licensing
- Security on the Internet
- Downloading Material from the Internet
- Supervision
- Recreational Use of the Internet
- Sanctions
- Legal Issues
- Acceptable use by pupils
- Cyber Bullying

- Inappropriate Material
- Acceptable Use of ICT within the Early Years Foundations Stage
- Early Years Developmental Profiles
- Acceptable use of ICT by EYFS practitioners and their managers
- Appropriate Use of Email
- Staff Code of Conduct for ICT

Aim

The Acceptable Use of ICT Policy will aim to:

- safeguard children and young people by promoting appropriate and acceptable use of information and communication technology (ICT).
- outline the roles and responsibilities of all individuals who are to have access to and/or be users of, work related ICT systems.
- ensure all ICT users have an acute awareness of risk, a clear understanding of what constitutes misuse and the sanctions that may be applied.

Roles and responsibilities

Registered person – DSL, Mrs Taggart, Deputy Head

Deputy Registered person - Head of STEAM and Computing, Mr Clifford

The registered person to have overall responsibility for ensuring online safety will be considered an integral part of everyday safeguarding practice. This will include ensuring:

- Early years practitioners and their managers will receive the appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Clear and rigorous policies and procedures are to be applied to the use/non-use of personal ICT equipment by all individuals who affect or come into contact with the early years setting.

  As a member of the school community, you should follow these principles in all your online activities:

  - Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
  - Do not access, create, or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, extremism or raises safeguarding issues).
  - Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
  - Do not access or share material that infringes copyright and do not claim the work of others as your own.
  - Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others or carry out illegal activities.

- Staff should not use their personal email or personal social media accounts to contact pupils or parents. Pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.
- Staff must verify all information from AI software to establish veracity before disseminating to children or other staff.

Using the School's IT Systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- Pupils are responsible for using the school IT systems in accordance with the E-safety Policy and for letting staff know if they see IT systems being misused. If pupils are accessing their email accounts, this should only be used for school related tasks such as projects and homework.
- The provision of school email accounts, Wi-Fi and internet access is for official school business, administration, and education.
- Staff and pupils should keep their personal, family, and social lives separate from their school IT use and limit as far as possible any personal use of these accounts.
- If a staff member's personal devices that include e-mail or apps that link to the School or Dukes are hacked or compromised, they must inform the DSL, Headmaster who will inform school staff immediately.

Passwords

Passwords protect The Lyceum's network and computer system are your responsibility. They should not be obvious and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed. You must change your password immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the school should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay.

Promoting Safe Use of ICT and the Internet

The school takes the importance of teaching pupils and staff to use ICT very seriously - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

The school has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies which help to reduce the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe, and the school will further promote safe use of ICT and the internet by educating pupils and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly.

Monitoring and Access

Staff, parents and pupils should be aware that school email and internet usage will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism, and the protection of others.

Personal devices are not permitted for the pupils. They have access to school technology, and this is managed by Compatibility.

Compliance with Related School Policies

All staff will ensure that they comply with the school's E-safety, Safeguarding, Anti-Bullying and Staff Code of Conduct Policies.

Acceptable use by parents and carers

A working partnership with parents and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable and unacceptable behaviour.

Should parents or carers wish to use personal technologies, such as cameras within the setting environment, the rules and regulations about taking photos on site are always explained. They are unable to access the school Wi-Fi network.

Acceptable use by visitors, contractors and others

All individuals who come into contact with the early years setting are expected to behave in an appropriate and respectful manner. No such individual will be permitted to have unsupervised contact with children and young people nor to use a mobile phone device. All guidelines in respect of acceptable use of technologies must be adhered to. The right to ask any individual to leave at any time is to be reserved. At school events, parents and visitors and during the day for contractors, if they have a concern, they must contact Mrs Sara Taggart, the school DSL at staggart@lyceumschool.co.uk and on a Thursday Mr Mike Stanley, Headmaster and DDSL at stanleym@lyceumschool.co.uk

Health and Safety

Since most ICT equipment is usually mains powered and may also be heavy, it represents a potential safety hazard and should be treated carefully. Portable equipment needs extra careful handling. In addition, most ICT equipment is Display Screen Equipment (DSE) and therefore falls under the relevant Health & Safety regulations.

As such, staff should follow the below guidelines

- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Do not move about the room while sitting on a chair.
- Any person who is found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer faults should be promptly reported to the Head of STEAM and Computing. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at the workstation.
- Mobile phones should not be used in the presence of children.
- At the end of a session:
- Log off/shut down according to instructions.
- Replace laptops as directed.
- Wind up and put away any headsets.

Retention of Digital Data

Staff and pupils must be aware that all emails sent or received on school systems may be kept in archive even if deleted. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. However, the work of pupils is cloud based through Google Classroom and Google Drive; this is monitored by Compatibility through Google Workspace and Google Admin.

Breach Reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data
- any external hacking of the school's systems, using malware
- application of the wrong privacy settings to online systems
- misdirected post or email
- failing to bcc recipients of a mass email
- unsecure disposal

The school must report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (within 72 hours) and certainly if it presents a risk to individuals. In addition,

controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, you should notify the Bursar and Head of Operations immediately.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the E-safety Policy, or if you are concerned that a member of the school community is being harassed or harmed online, you should report it to a member of SLT or to the Safeguarding Governor for The Lyceum. Reports will be treated in confidence.

Security and Software Licensing

Security is especially important in schools, where vigilance is always needed to be ready to detect any forms of personal intimidation and exposure to inappropriate material. It is therefore very important that users' accounts are used only by themselves; otherwise, they are exposed to impersonation by another user.

The following rules are industry standard:

- Always log out of your computer when you have finished, or if you must leave it unattended.
- Do not let anyone else log in to a computer using your username and password.
- Do not tell anyone your password; you are responsible for keeping it secure.

The school uses up-to-date antivirus software on all computers; however, antivirus software is only as good as the latest virus definitions, which always lags the discovery of new virus threats. Therefore:

- Users must report any virus alerts they encounter to the Head of Computing.
- Users must report anything suspicious to a member of the SLT.

Installing software onto the school's computers is very carefully controlled and audited by the ICT technician, in order that the school can be sure to be acting legally by not breaking licensing and copyright laws in respect of software. In addition, uncontrolled installation of software represents an unacceptably high security risk. Staff are not permitted to install software or programmes onto computers without the prior authorisation of the Head of STEAM and Computing.

Security on the Internet

The Internet can be a dangerous place. Not only can it provide access to material which might be considered inappropriate for certain audiences, but it can also be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this:

- Do not type any personal details (including your name or email address) onto a web site unless you are sure of the authenticity and trustworthiness of the associated company.
- The use of chat rooms is prohibited.
- The use of Instant Messaging is prohibited.
- The use of Internet-based email or newsgroups is prohibited except with the prior written approval of the headmaster.

Downloading Material from the Internet

Most material on the Internet is covered by copyright law and, unless specifically stated otherwise on the web site, users may be breaking the law by downloading material.

Do not download or copy any material from the Internet unless you are sure that the source is reliable and that there is no copyright, intellectual property right or licensing restrictions. If in doubt, ask the Head of STEAM and Computing. In addition, it has already been stated in this policy that installation of software is prohibited.

Supervision

Access to the Internet will be blocked to pupils outside of normal classes (i.e. during lunchtimes and after school). Pupils may be unblocked for a specific lunchtime or after-school session if a suitable justification for requiring access to the Internet is accepted and there is a member of staff available to supervise. During normal lesson time it is expected that staff will supervise access to the Internet.

Recreational Use of the Internet

Access to the Internet is provided to support the curriculum, support school administration and for staff professional development only.

Recreational or personal use of the Internet is not permitted during lesson time except with the prior written approval of the headmaster. It will be considered a disciplinary issue if staff access the Internet for personal use during lesson time. Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.

Sanctions

Pupils/Staff found not to be abiding by this policy may be subject to sanctions. Violations of the school's E-Safety and acceptable Use of ICT Policy will result in a temporary or permanent ban on your use of the school network or of the internet. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour. When applicable, the school may be under obligation to involve police or local authorities.

Legal Issues

The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any programme or data held in any computer". The school wishes to make it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised".

This policy has been drawn up taking into account The Education [Independent School Standards] Regulations 2014 and Keeping Children Safe in Education 2025 as well as the school's own staff code of conduct.

Other DFE guidance is taken from Teaching online Safety in schools 2023 and DFE Digital Standards 2025.

Acceptable use by pupils

Pupils will only be able to download a file under the direct supervision of a member of staff, and it will be virus checked prior to being opened. The use of game-style activities and websites should be monitored by practitioners to determine suitability.

Should a pupil be found to misuse ICT inappropriately, the following sanctions will be applied:

• **Step 1:** Should it be considered that a c has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be suspended from a particular activity.

• **Step 2:** If there are to be further incidents of misuse, the pupil will be suspended from using the internet or other relevant technology for an increased period. The parent or carer will be invited to discuss the incident in more detail with the DSL or headmaster, and the most appropriate course of action will be agreed.

• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. If misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a pupil be considered at risk of significant harm, the Safeguarding Policy will also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Services.

If a pupil should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

Cyber Bullying

The Safeguarding, Anti – Bullying and Behaviour Policies contains up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber bullying. It should be recognised that all inappropriate behaviour will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world, and this is to be reflected in all relevant policies.

Inappropriate Material

The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden. The school reserves the right to monitor or inspect any programmes, files or other data stored on the school's ICT equipment for suitability.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Acceptable Use within the Early Years Foundations Stage

Early years practitioners and their managers will ensure:

- the timely reporting of concerns in relation to alleged misuse or known incidents, subject to agreed procedures.
- ICT equipment is to be checked before use and all relevant security systems judged to be operational.
- awareness will be raised of any new or potential issues, and any risks which could be encountered.
- EYFS pupils are to be supported and protected in their use of online technologies – enabling them to use ICT in a safe and responsible manner.
- online safety information is to be presented to EYFS pupils as appropriate for their age and stage of development.
- EYFS pupils will know how to recognize and report a concern.
- all relevant policies and procedures are to be always adhered to, and training undertaken by EYFS staff.
- The importance of online safety in relation to safeguarding is to be understood by all ICT users and the training, learning and development requirements of early years practitioners are to be monitored, and additional training needs identified and provided for.

Early Years Developmental Profiles

Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form of recording their progression in the Early Years Foundation Stage and other areas of the school. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care. When pupils join The Lyceum, we ask parents to sign consent for photographs and videos to be taken for such purposes.

Acceptable use of ICT by EYFS practitioners and their managers

Early years practitioners and their managers should be enabled to use work-based online technologies:

- to access age-appropriate resources for children and young people.
- for research and information purposes
- for study support.

All EYFS practitioners and their managers will be subject to authorised use as agreed by the DSL. Authorised users will have their own individual password to access a filtered internet service provider. Users are not generally permitted to disclose their password to others, unless required to do so by law or are requested to do so by the DSL. All computers and related equipment are to be locked when unattended to prevent unauthorised access. All EYFS practitioners and their managers are to be provided with a copy of the Acceptable Use of ICT Policy. The use of personal technologies will be subject to the authorisation of the DSL for Safeguarding, and such use will be open to scrutiny, monitoring and review.

Should it be alleged that an EYFS practitioner is to have misused any ICT resource in an abusive, inappropriate or illegal manner, a report is to be made to the DSL immediately. Should the allegation be made against the DSL, a report is to be made to the headmaster. Procedures are to be followed as appropriate, in line with the Safeguarding Policy and/ or Disciplinary Procedures. Should allegations relate to abuse or unlawful activity, Children's Social Care, the Local Authority Designated Officer, Ofsted and/or the Police will be notified as applicable.

Appropriate Use of Email

- This section applies to all staff members within the school.
- This includes peripatetic musicians, external agency staff and volunteers working in the school and to all staff members who work during before and after school clubs, holiday clubs and all other activities provided by the school, inclusive outside of the normal school hours.
- This policy is made available to parents, staff and pupils on the website.
- This policy will be subject to continuous monitoring, refinement and audit by the headmaster.
- The headmaster will undertake a formal annual review of this policy for the purpose of monitoring or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.
- Email should always be written carefully and politely and should always be treated as a public medium.
- Sending emails containing offensive, defamatory or harassing material is strictly forbidden.
- If you receive unsolicited, disturbing, offensive or harassing content in an email, inform the Bursar and Head of Operations immediately.
- The creation or forwarding of chain letters is prohibited.
- The school will provide email accounts for staff and pupils requiring them for legitimate purposes.
- The school uses antivirus software to detect viruses in emails and will continue to investigate suitable software to filter unsuitable or unsolicited email entering the school's mail system.
- The school reserves the right to scan all incoming and outgoing email content for the purpose of verifying the performance of filtering/security software and adherence to the school's policies.
- However, antivirus software is only as good as the latest virus definitions, which always lag the discovery of new virus threats. Staff and pupils will be taught how to configure the email reading programme used by the school (Office365) such that the subject and sender's name only may be viewed before deciding whether to read the email or delete it – this avoids automatically viewing the content of emails.

- Do not open or read email unless you recognise the sender or are sure it is from a legitimate source.
- Never open or save an email attachment unless you are sure of the sender and the source and purpose of the attachment.
- It has become very common now for emails to be “spoofed”, meaning that the apparent author is not the real author of an email. Such emails are usually the result of a PC which contains your email address becoming infected with a virus.
- Do not automatically assume that received email has been sent by the person it says it is from.
- Do not click on web links inside an email unless you are sure of the source of the email.
- Use of email is provided to support the curriculum, support school administration and for staff professional development only. Recreational or personal use of the school’s email system is not permitted except with the prior written approval of the headmaster.

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's E-safety policy and Acceptable Use of ICT Policy for further information and clarification.
All members of staff are required to read and sign the Staff Code of Conduct for ICT and these will held on file by the Headmaster.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet/ Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the headmaster.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDA's, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on iSAMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the headmaster.
- I will not install any hardware of software without permission from the headmaster.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school's policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headmaster.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the headmaster.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will not store parents' or pupils' phone details on my personal device, and I will only contact parents via school email or school phone devices.

User signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school and understand that failure to do so may lead to disciplinary actions or dismissal.

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

Full Name..... (printed)

Job title.....



