E-Safety Policy

Date reviewed	May 2020
Frequency	Annually
Next review date	June 2021
Reviewed by	Academic Standards, Safeguarding, SEN and Educational Trips Committee

Signed:..... Dated: 7/5/2020

Chair of Governors

Signed:..... Dated: 7/5/2020

CONTENTS

AIMS

Goldington Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

LEGISLATION AND GUIDANCE

- Keeping Children Safe In Education DFE 2019
- The Prevent Duty DFE 2015
- Preventing and Tackling Bullying DFE 2017
- Education Act 2011
- Equality Act 2010
- National Curriculum Programmes of study for Computing
- Data Protection Act (GDPR) 2018
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Lawful Business Practice Regulations 2000

INTRODUCTION

This policy has been developed to ensure that all adults in Goldington Academy are working together to safeguard and promote the welfare of children and young people.

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained through the use of ICT, whilst minimising any associated risks. It prescribes actions that will be put in place to address any concerns about child welfare and safety, and to protect children, young people and staff from risks and infringements.

This policy complements and supports other relevant school and Local Authority policies.

The purpose of internet use in school is to help raise educational standards, promote pupil achievement, enable pupils to establish good internet practice, support the professional work of staff, and enhance the school's management information and business administration systems.

The internet is an integral part of 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

ETHOS

It is the duty of the school to ensure that every child and young person in its care is safe. This expectation also applies to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

All staff have a responsibility to support e-Safety practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols.

E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Child Protection and Safeguarding policy, Anti- Bullying and Behaviour Policies and may be referred to the police.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy.

ROLES AND RESPONSIBILITIES

The Principal of Goldington Academy will ensure that:

- Staff understand this policy, and that it is being implemented consistently throughout the school
- All staff should be included in e-safety training. Staff must also understand that misuse of the internet (e.g. adult or explicit material, incitement, gambling, etc) may lead to disciplinary action and possible dismissal.
- Director of IT services receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding/Network Manager.
- All temporary staff and volunteers are made aware of the school's e-safety Policy and arrangements.
- A commitment to e-safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body of the school will ensure that:

- All governors have read and understood this policy
- All governors agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- There is a member of the school's staff who is designated to take the lead on e- safety within the school.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

- There is a member of the Governing Body who is designated to take responsibility for safeguarding, including e-safety.

The Director of IT Services will:

- Act as the first point of contact with regards to breaches in e-safety and security.
- Liaise with the Designated Person for Safeguarding as appropriate.
- Ensure that ICT security is maintained.
- Attend appropriate training.
- Provide support and training for staff and volunteers on e-safety.
- Ensure that all staff and volunteers have received a copy of the school's 'Acceptable Use of ICT' document.
- Ensure that all staff and volunteers understand and are aware of the school's e-safety Policy.
- Ensure that the school's ICT systems are routinely reviewed with regard to security.
- Conduct a full security check and monitoring the school's ICT systems on a regular basis
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy DSL are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy and anti-bullying policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Detail issues relating to online safety in school to the principal and/or governing board via the termly safeguarding report as necessary.

EDUCATING PUPILS

Developing good practice in internet use as a tool for learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.
- Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.
- Pupils will be taught to respect the rights of copyright holders.
- Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its reliability, particularly at KS3.
- Rules for internet access will be posted in all rooms where computers are used.
- Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks during lesson using the internet.
- Pupils will be taught about how internet use is monitored and what the consequences for misuse could be.
- Responsible internet use, covering both school and home use, will be included in the PSHE curriculum

SUPPORTING PARENTS/CARERS

Parents/carers will be informed of the school's Internet Policy which may be accessed on the school website.

Any issues concerning the internet will be handled sensitively to inform parents/carers without undue alarm.

Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/carers.

Interested parents/carers will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

Opportunities will be offered to parents to update their knowledge of safe internet use through external agencies such as the Police. These opportunities depend very much on the availability of external agencies to deliver such opportunities.

DATA SECURITY

The Principal has overall responsibility for ensuring there is adequate control over data security. Any suspected breach of security should be reported immediately to the Principal and/or Senior Teacher responsible for Safeguarding.

Any incidents relating to the confidentiality of information shall be recorded in an incident log. The incident log shall be reviewed termly by the Senior Leadership Team.

Access to all ICT systems should be via unique login and password. Passwords should be kept confidential and should be changed regularly. All members of staff with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords. E.g. keeping their password secure from pupils, family members and other staff; using different passwords for accessing school systems to that used for personal purposes; adding numbers or special characters; changing passwords regularly.

Where possible, all information storage will be restricted to only necessary users. If access needs to be granted to new users it will be approved by the Principal and/or Senior Teacher responsible for Safeguarding.

Pupils' sensitive (restricted) information shall not be stored on any mobile device unless encrypted.

When using memory sticks, staff should ensure that no personal data or photographs exist on the memory stick. Staff must ensure that memory sticks are encrypted if they are to hold photographs/video/data relating to pupils.

Computers should be logged off when left unattended, including staff work room.

When staff leave Goldington, their passwords and remote access to the schools computer systems shall be disabled, in a timely manner.

Staff will receive appropriate training on Data Security.

MANAGING ELECTORNIC COMMUNICATION

Personal e-mail or messaging between staff and pupils should not take place.

Staff must use a school e-mail address or Show My Homework if they need to communicate with pupils about their school work e.g. homework, etc.

Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail.

Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

Access in school to external personal e-mail accounts may be blocked. Pupils and staff will be encouraged to use their school provided e-mail accounts.

The forwarding of chain letters is not permitted.

Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

MANAGING WEBSITE CONTENT

Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

Photographs of pupils will **not** be used without the written consent of the pupil's parents/carers. The names of pupils will **not** be used on the website in association with any photographs.

Work will only be used on the website with the permission of the pupil and their parents/carers.

The point of contact on the school website will be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.

The Principal or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing.

Photographs used on the site will be carefully selected to limit the risk of them being misused.

The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

SOCIAL NETWORKING AND CHAT ROOMS

The school will control access to moderated social networking sites and educate pupils in their safe use.

- Staff must not exchange social networking addresses or use social networking sites to communicate with pupils or parents.
- Pupils will **not** access unmoderated social networking sites eg 'Snapchat', 'Instagram' 'Facebook', 'WhatsApp' or 'Pinterest'.
- Pupils will be taught the importance of personal safety when using social networking sites and chat rooms.
- Pupils will **not** be allowed to access public or unregulated chat rooms.

- Pupils will only be allowed to use regulated educational chat environments and use will be supervised.
- Pupils will be advised to use nick names and avatars when using social networking sites.

Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a pupil is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

USE OF MOBILE DEVICES IN SCHOOL

Pupils

Mobile devices will not be in a pupil's possession during school hours. Phones and other mobile devise must be handed in to the correct box for safe storage during the day. Devices can then be collected by pupils at the end of the school day.

If a mobile device is found in a pupil's possession during the day then:

- The device will be confiscated and safely stored
- The pupil's parents will be informed and will be asked to collect the phone
- Following multiple breaches of this rule, the school may no longer allow the individual pupil to bring their phone on to the school site

The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's Anti-Bullying and Behaviour Policies.

Staff

Mobile phones will not be used by staff during registration or lesson time. However, if required to do so due to special circumstances, staff can request permission from a member of the senior leadership team who may grant permission. Under no circumstances should personal phones or cameras be used to photograph or record children, timing children for sports events, or for any other application.

Staff who have been issued a school mobile phone should have this in their possession during the school day and may use it as necessary to ensure the safe running of the school.

FILTERING

The school will work in partnership with parents/carers, the Local Authority, the DfE and the Internet Service Provider to ensure systems that protect pupils and staff are reviewed and improved regularly.

If staff or pupils discover unsuitable sites, the URL **(address)** and content must be reported to the Director of IT Services / Network Manager / Principal immediately.

Any material the school deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwf.org.uk).

Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable

Filtering methods will be selected by the school in conjunction with the LA and will be age and curriculum appropriate.

AUTHORISING INTERNET ACCESS

All staff must read and sign the school's 'Acceptable use of ICT' document before using any school ICT resources and any staff not directly employed by the school will also be asked to sign the school's 'Acceptable Use of ICT Resources' document before being allowed internet access from the school site.

The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

The school will maintain a record of pupils whose parents/carers have specifically requested that their child be denied internet or e-mail access.

Parents/carers will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document and give permission for their child to access ICT resources.

Staff will supervise access to the internet from the school site for all pupils.

PHOTOGRAPHIC, VIDEO AND AUDIO TECHNOLOGY

It is not appropriate to use photographic or video technology in changing rooms or toilets.

Staff may use photographic or video technology to capture and support school trips and appropriate curriculum activities.

Audio and video files may not be downloaded by pupils without the prior permission of the Director of IT Services / Network Manager

Videoconferencing and webcam use will be appropriately supervised for the pupil's age.

ASSESSING RISKS

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The Senior Leadership Team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimise risks will be reviewed regularly.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The Principal will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

Access to any websites involving gambling, or financial scams is strictly forbidden and will be dealt with accordingly.

MONITORING

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

All internet activity is logged by Impero and is managed by the Director of ICT and the Network manager. The school's internet provider also logs the school's internet activity. These logs may be monitored by the Principal and Governing Body.

Staff mailboxes are regularly audited, specifically focusing on staff to pupil communication.

CONSULTING STAFF

It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies:

- All staff are governed by the terms of the school's 'Acceptable use of ICT' document and will be provided with a copy of the School Internet Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction.

- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise members of staff who operate the monitoring procedures.

MAINTAINING ICT SECURITY

Personal data sent over the school network will be encrypted or otherwise secured.

Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

The Network Manager will ensure that the system has the capacity to deal with increased traffic caused by internet use.

STAFF USE OF WORK DEVICES OUTSIDE OF SCHOOL

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

RESPONDING TO ISSUES OF MISUSE

Staff, children and young people, parents/carers must know how and where to report incidents and the action that school will take in response to incidents. Parents/carers and pupils will work in partnership with the school staff to resolve any issues.

Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will be dealt with in accordance with the school's Child Protection and Safeguarding policy, Anti- Bullying and Behaviour Policies and may be referred to the police.

Complaints related to child protection will be dealt with in accordance with the school's Safeguarding Policy. Incidents of a serious nature may result in referrals to external agencies, e.g. the Police, the Channel Panel, Bedford Borough MASH, Bedford Borough Early Help. If

appropriate, early contact with such agencies should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

- Mobile devices being confiscated – parents will be informed and asked to collect from the school office
- Interview/counselling by an appropriate member of staff
- Informing parents/carers
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system
- Referral to the outside agencies
- Loss of other privileges in school
- Internal isolation

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Director of IT Services / Network Manager. A log of any unsuitable sites will be kept by the Director of IT Services. See form in Appendix A.

LINKS TO OTHER POLICIES

- Behaviour policy
- Anti-bullying policy
- Equality Policy
- Whistleblowing policy
- Staff disciplinary procedures
- Child Protection policy
- Complaints policy

ICT- PUPIL ACCEPTABLE USE AGREEMENT

As a parent/guardian, I will ensure my child(ren) have read and understood the following requirements:

- I will only use a computer when supervised by an adult.
- I will only use ICT in school for school purposes.
- I will not download or install software on school equipment.
- I will only use my school email address.
- I will not tell other people my ICT passwords.
- I will only open email attachments from people I know, or my teacher has approved.
- I will make sure that all ICT communications with pupils and adults are responsible, polite and sensible.
- I will be responsible for my behaviour when using the internet (this includes the resources I access and the language I use).
- I will not deliberately search for, download or send material that could be unpleasant or offensive. If I accidently come across such material I will report it immediately to my teacher.
- I will not give out any personal information such as my name, phone number or address.
- I know that my use of ICT can be checked and that my parent/carer can be contacted if a member of school staff is concerned about my e-Safety.
- I will not publish pictures of school peers without their permission.
- I understand that these rules are designed to keep me safe, and that if they are not followed school sanctions will be applied and my parent/carer may be contacted.

ICT- OBLIGATIONS FOR GOLDINGTON ACADEMY

Goldington Academy commits to the following steps to safeguard children with respect to use of ICT:

- Goldington Academy will put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained through the use of ICT, whilst minimising any associated risks.
- Goldington Academy will appoint a Designated Member of Staff for e-safety.
- All staff will read and sign the school's ICT Acceptable Use Policy for all adults working at Goldington Academy. Any staff found to have contravened any of the requirements may face disciplinary action.

Engaging minds. Nurturing success. Inspiring futures.

GOLDINGTON ACADEMY

Haylands Way, Bedford MK41 9BX
Telephone: 01234 261516 **Fax:** 01234 272344
e-mail: office@goldington.beds.sch.uk
Website: www.goldingtonacademy.org.uk
Principal: Mr. Francis Galbraith BSc (Hons), NPQH, MBA

Dear Parent/Carer,

Re. ICT Acceptable Use Policy (AUP)

ICT including the Internet, learning platforms and email have become an important part of learning in our school. We expect all pupils to be safe and responsible when using any ICT. It is essential that pupils are aware of e-Safety and know how to stay safe when using ICT.

The school has devised an 'ICT Acceptable Use Policy' (see overleaf) to ensure that everyone stays safe and has a positive experience when using ICT. Please read through the policy and discuss the rules with your child. By returning the attached form signed by you and your child, you are accepting the rules for ICT usage in school.

We would like all pupils to have access to the same resources and we are asking for your parental consent so that your child can use the Internet whilst at school. If we do not receive the consent form, your child will not be able to use the full resources available to them.

If you have any queries, then please contact your child's class teacher or Mr Latchman, Head of Computing Science / Director of IT Services.

Please return the form to school as soon as possible for our records.

Yours sincerely

M Latchman

Mr M Latchman Head of Computing

✂----------

ICT Acceptable Use Policy

I/We give permission for (pupil name) to use the Internet at school for educational purposes.

I/We have discussed this document and (pupil name) agrees to follow the e-Safety rules and support the safe and responsible use of ICT at Goldington Academy.

Parent/Carer Signature: Date:

Pupil Signature: Date:

ICT Acceptable Use Policy for all adults working at Goldington Academy

The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring.

All adults using ICT equipment within the school must ensure that they have read and abide by the Acceptable use Policy. If they are found to have contravened any of the requirements they may face disciplinary action.

The school's ICT systems and network should be used primarily for school purposes but **occasional** personal use is permitted during 'non-contact' time and out of school hours. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

ICT equipment

- I will not give anyone access to my login name or password (unless authorised by the Principal)
- I will not attempt to introduce any unlicensed applications
- I will not corrupt, interfere with or destroy any other user's information
- I will not release any personal details of any colleague or pupil over the internet, particularly on social networking sites such as 'Facebook', 'Instagram', 'WhatsApp' etc.
- I will not use the school internet access for business, profit, advertising or political purposes
- I will not leave my account open at the end of a session
- I will not engage in any activity which might compromise the security of the school network
- I will not install, attempt to install or store programs of any type without permission of the Director of IT Services / Principal / Network Manager.

E-mail

- E-mails should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny.
- I will not include offensive or abusive language in my messages or any language which could be considered defamatory, obscene or menacing.
- I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- I will make sure that nothing in messages could be interpreted as libellous.
- I will not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- I will not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.
- I will never open attachments to e-mails unless they come from someone I know and trust.

Internet

- I will watch for accidental access to inappropriate materials and report any offending site to the Director of IT Services/Network Manager and Principal so that action can be taken.
- I will check copyright before publishing any work and ensure that any necessary permission is obtained.
- I will ensure that the school's photo policy is strictly adhered to.
- I will report any breaches of the Internet policy to the Director of IT Services / Network Manager / Principal

Mobile Phones

- I will not use my mobile phone during lesson or registration times. If required to do so, due to special circumstances, I will get permission from a member of SLT.

Print Name:

Signature: **Date:**