E-Safety Policy

Date reviewed	January 2026
Frequency	Annually
Next review date	February 2027
Reviewed by	Health & Safety, Premises and Safeguarding Committee

Signed:...   Dated: 05/02/2026

Chair of Governors

Signed:...   Dated: 05/02/2026

Principal

CONTENTS

AIMS

Goldington Academy aims to:

- Haverobust 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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools

- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff

- Relationships and sex education –

- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

- It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate

images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

- The policy also takes into account the National Curriculum computing programmes of study.

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 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 governing body

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the Principal, Network manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school child protection policy

- 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

- Updating and delivering staff training on online safety

- Liaising with other agencies and/or external services if necessary

The School Business Manager

The School Business Manager, in conjunction with the IT Technician, is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy

- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

- Parents can seek further guidance on keeping children safe online from the following organisations and websites:

    National Online Safety

    What are the issues? – UK Safer Internet Centre

    Hot topics – Childnet International

    Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

EDUCATING PUPILS

Developing good practice in internet use as a tool for learning is essential.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

- Pupils will complete E Safety training through the Online Safety Alliance

- Pupils will learn about the safe and responsible use of Artificial Intelligence (AI) software with its different functionalities and key limitations.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

- How to report a range of concerns

By the end of their time at Goldington Academy, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

- What to do and where to get support to report material or manage issues online

- The impact of viewing harmful content

- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail

- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

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.

Opportunities will be offered to parents to update their knowledge of safe internet use through support tools, such as National Online Safety.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes assemblies, form tutor period, Life Skills etc.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. This is mostly through National Online Safety.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The principal, and any member of staff authorised to do so by the principal, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Principal.

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or

- Undermine the safe environment of the school or disrupt teaching, and/or

- Commit an offence

If inappropriate material is found on the device, it is up to the Principal to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or

- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on <u>sharing nudes and semi-nudes: advice for education settings working with children and young people</u>
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they must be handed in to the Small Hall at the beginning of the school day and must not be carried or used during the school day.:

Mobile phones will be confiscated if found in the possession of pupils during the school day. Parents will be asked to collect the phone from the school office,

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the School Business Manager.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on E Safety.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

Children can abuse their peers online through:

- o Abusive, harassing, and misogynistic messages
- o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- o Sharing of abusive images and pornography, to those who don't want to receive such content

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

Develop better awareness to assist in spotting the signs and symptoms of online abuse

Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

The following appears in the Home School Agreement document which all new pupil and parents receive digitally. Parents are asked give consent to the acceptable use of ICT within school as part of the Home School Agreement.

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' 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.
https://www.goldington.beds.sch.uk/policies/policies.

If you have any queries, then please contact your child's form teacher or Mr Atkinson, Designated Safeguarding Lead.

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 not bring in/use any form of portable storage devices such as a USB drive or portable hard drive
- 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

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 School Business Manager / Principal / IT Technician.

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 School Business Manager/IT Technician 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 School Business Manager / IT Technician / 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:** _____