GOTHIC MEDE ACADEMY ONLINE SAFETY (INCLUDING ACCEPTABLE USE) POLICY

DATE: September 2022

REVIEW DATE: September 2023

COMPUTING LEAD TEACHER: Michael Warlow

DSL: Jennifer Milligan

DDSLs: Thomas Clarke, Nicola Davis, Alison Sugden, Julie Undrell

SAFEGUARDING GOVERNOR: Trudie Squires

1. AIMS

Gothic Mede 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

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) 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 headteachers 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.

3. ROLES AND RESPONSIBILITIES
3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the principal to account for its implementation. The safeguarding governor will meet with the DSL on at least a termly basis to discuss online safety.

The safeguarding governor is **Trudie Squires.**

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 (appendix 2)

3.2 The Principal

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our 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 and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 3) 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 academy's behaviour policy
- Liaising with other agencies and/or external services if necessary
- Providing updates on online safety in school to the principal and/or governing board
- Receiving, reviewing and acting upon (if appropriate) the weekly staff and pupil 'suspicious search queries' reports from Netsweeper

This list is not intended to be exhaustive.

3.4 The Computing Lead Teacher (via Partners In Education)

The Computing Lead Teacher is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 security checks and regularly monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

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

- Maintaining an understanding of this policy
  - Policy is available on website
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the academy's ICT systems and the internet (appendix 2), and ensuring that pupils follow the academy's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy

This list is not intended to be exhaustive.

3.6 Parents / Carers

Parents/carers are expected to:

Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (appendix 1)

Read, sign and agree to the terms on acceptable use of the academy's ICT systems and internet for their child (appendix 1)

Ensure their child understands and follows what is expected of them if they bring a device with them to the academy that can access the internet.

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and Members of the Community

Visitors and members of the community who use the academy'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 (appendix 2).

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

Gothic Mede Academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE), Computing programmes of study and a planned programme of assemblies.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating learners in the effective use of the internet to research (including the skills of knowledge location, retrieval and evaluation) and to respect copyright when using material accessed on the internet.
- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.1 Acceptable Use Policies

Our schools will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology in accordance with our Behaviour Policy
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches

4.2 Digital Literacy

As part of the Computing Curriculum, our schools deliver discrete teaching of digital literacy and citizenship skills in supporting pupils to act responsibly and develop pupils' understanding of online safety.

At Gothic Mede Academy we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

4.3 Vulnerable Learners

Gothic Mede Academy recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Gothic Mede Academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

When implementing an appropriate online safety policy and curriculum, Gothic Mede Academy will seek input from specialist staff as appropriate, including the SENCO and LAC Designated Teacher.

5. EDUCATING PARENTS ABOUT ONLINE SAFETY

The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via our website. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL. The school will regularly arrange for the police to brief parents on e-safety.

6. CYBER-BULLYING

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the academy's behaviour policy.)

6.2 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.

Academy staff will discuss cyber-bullying with pupils, where age appropriate, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff will use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 13 for more detail).

The academy will signpost information about cyber-bullying to parents / carers so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the academy's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

Gothic Mede Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any academy rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

In cases where inappropriate material is found on electronic devices, the academy will aim (if appropriate to do so) to inform parents /carers.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

7. ACCEPTABLE USE OF THE INTERNET IN THE ACADEMY

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet (appendices 1-2). Visitors will be expected to read and agree to the academy's terms on acceptable use (if relevant). Use of the academy'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 in appendices 1 and 2.

8. PUPILS USING MOBILE DEVICES IN THE ACADEMY

Older pupils who are travelling to and/or from school independently may bring mobile devices into the academy, but are not permitted to use them or have them out on show during:

- Lessons
- Break and lunchtimes
- Walking around the academy site / grounds
- Clubs before or after school, or any other activities organised by the academy

Pupils are required to hand their mobile device to a member of office staff during morning registration or when asked to do so. Pupils will have their mobile devices returned to them when they have finished their school day. Any breach of the acceptable use agreement by a pupil will trigger disciplinary action in line with the academy's behaviour policy, which may result in the confiscation of their device. If a mobile device is confiscated from a pupil, it will be held securely and will have to be collected by the parent / carer at the end of the school day.

9. STAFF USING MOBILE DEVICES IN THE ACADEMY

Staff may bring their mobile devices to school on the understanding that the device:

- Is kept out of sight when in the presence of pupils
- Is used only in the staff room or in office spaces when no pupils are present
- Is not used to take photos or videos of pupils unless permission from the Principal is sought and obtained in advance. Any images or videos must be deleted as soon as possible in the presence of a member of SLT.
- Staff should always use the academy's devices to take photos and videos of pupils.

Staff may use their mobile phones during emergency situations, or on school trips. The use of these around the children should be kept to a minimum.

The section "Staff Use of Mobile Telephones" in the BEST Staff Code of Conduct should be referred to for guidance in this area.

10. VISITORS USING MOBILE DEVICES IN THE ACADEMY

Visitors may bring mobile devices to the academy but they must be kept out of sight whilst they are on site and when pupils are on site. If a professional (such as a social worker) wishes to use their mobile device, it must be used in a staff office space or staff room when there are no pupils present and a member of staff should be informed.

11. STAFF USING WORK DEVICES OUTSIDE THE ACADEMY

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 – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device is locked when unattended.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 2. Staff must use their work devices solely for work activities.

If staff have any concerns over the security of their device, they must report their device to a Partners in Education representative in order to seek their advice and support.

12. HOW THE ACADEMY WILL RESPOND TO ISSUES OF MISUSE

Where a pupil misuses the academy's ICT systems or internet, the academy will follow the procedures set out in our behaviour policy. 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 academy'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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

13. TRAINING

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. 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).

The DSL and deputies 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.

14. MONITORING ARRANGEMENTS

Staff members must log behaviour and safeguarding issues related to online safety on CPOMS. These reports will be reviewed and monitored by the DSL and their deputies.

The DSL will receive, review and act upon (if appropriate) the weekly staff and pupil 'suspicious search queries' reports from Netsweeper.

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

15. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- GMA Safeguarding policy incl. child to child abuse
- GMA Behaviour and discipline policy
- BEST Staff code of conduct
- BEST GDPR policy and privacy notices
- GMA Complaints procedure
- GMA Anti-bullying Policy

Pupil Acceptable Use Policy Agreement – Early Years/Key Stage 1

This Acceptable Use Policy

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

This is how we stay safe at Key Stage 1 when we use computers:

- I will ask a teacher / an adult if I want to use the computer.
- I will only use activities that the teacher /an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from the teacher / an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher / an adult if I see something that upsets me on the screen.
- I know not to chat to anyone online.
- I will keep my personal information and passwords safe.
- I will always be nice if I do post or put up messages online.
- I know that if I break the rules I might not be allowed to use the computer.

All pupils need to write their name in the box below to show that they have heard, read, understood and agree to the Pupil Acceptable Use Agreement.

I understand the Pupil Acceptable Use Agreement:

Name:		Class:	

<u>Pupil Acceptable Use Policy Agreement – Key Stage 2</u>

This Acceptable Use Policy

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

Personal Safety

- I will keep my passwords safe and will not use other people's passwords
- I will be aware of "stranger danger", when working online.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material; messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will report any bad behaviour by telling a responsible adult
- I know that the school can look at my use of ICT and see the footprint of what I use online ICT Property and Equipment
- I will respect all computer equipment and will report any damage or faults.
- I will respect others' work and will not access, copy, move or remove files.
- I will not use mobile phones/USB devices in school.
- I will not use any programs or software without permission.
- I will not use or open email, unless I know and trust the person or organisation.
- I will not install programs or alter any computer settings.

Cyber Bullying

- I will be polite when I communicate with others
- I know not to do online what I wouldn't do offline (like in the playground)
- I will not use inappropriate language or make unkind comments
- I appreciate others may have different opinions
- I will not upload or spread images of anyone

The Internet

- I understand that I need permission to be on the Internet.
- I will not fill in any online forms without adult permission
- I will not use any sites I've not had permission to use, this includes social media sites that I'm not old enough to use
- I will learn about copyright laws and make sure I acknowledge resources
- I will not upload or download images, music or videos without permission

- I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

Mobile Phones

- I know that mobile phones are not allowed to be used during the school day and are advised to be left at home, if brought to school it must be switched off and given to my class teacher.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phones or personally-owned mobile devices without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

Outside of the School Community

- I understand that this agreement is for in and outside the school
- I know there will be consequences if I am involved in incidents of inappropriate behaviour covered in this agreement which maybe a police matter.

All pupils need to sign in the box below to show that they have read, understood and agree to the Pupil Acceptable Use Agreement.

I understand the Pupil Acceptable Use Agreement for using technology, internet, email and online tools safely.

Name:		Class:	

APPENDIX 3 – AUP PARENTS/CARERS

Parent/Carer E-Safeguarding and Acceptable Use Policies Information

As part of the programme of activities in school, all pupils have the opportunity to access a wide range of communication technology resources. These resources are an essential part of promoting children's learning and development; however, we also recognise the potential risks associated with these technologies. We therefore have an E-Safeguarding and Acceptable Use Policies in place in school.

In recent years, social networking sites such as Facebook and Twitter have grown in popularity and many people use them to communicate with family and friends, as we do to our school family. The vast majority of people who use social networking show respect in their communication with others and is something we must encourage to show our children that we are positive 'digital role models'. However, there are times when people disregard the rules and will use social networking sites to cyberbully and harass others.

Recently, there have been a number of high-profile cases in the media where people have used the internet to intimidate and bully others. The police have investigated these cases and in some instances have led to criminal prosecutions.

As a school, we encourage our parents to support us with the education and wellbeing of their children and if at any time, parents feel they have issues regarding their child's education or with school matters, they should see their class teacher. If the issue has not been resolved, then an appointment can be made with the Principal. We also have a complaints policy on the school website if deemed necessary.

If an incident is reported to school staff, it should be investigated and, if school deem it appropriate, will be acted upon by the school's Principal. In extreme cases, the Principal would consider whether it appropriate to notify the police or solicitors to take further action.

Therefore, as a Parent/Carer, you are asked to:

- Read the Parent/Carers Acceptable Use Agreement
- Read and talk to your child about their Pupil Acceptable Use Agreement
- Parent/Carer and child to sign their agreements.
- Return one signed copy of the agreement to School and keep a copy to refer to.

If you disagree with any of the rules within the agreements or feel there is an area of Internet Safety you feel is not being developed, please contact the Head teacher.

Please remember, all children in school are taught how to keep safe and be responsible when they are online, whether they are at school or at home. As children are able to access the internet outside school, whether this is at home, a friend's house or on a mobile device, we need to work in partnership with you the parent/carer to keep our children safe.

Parent / Carer and Pupil Acceptable Use Agreement Form

Parent / Carer Acceptable Use Agreement:

- I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials through a managed filtered system.
- I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.
- I understand that my son's/daughter's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Internet Safety Rules or Pupil Acceptable Use Agreement.
- I understand not to upload any photos of Gothic Mede Academy pupils, that are not my own, at any school event (for example, assemblies'/sports days/plays or school trips) onto a social media site.
- I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate or malicious comments about the school or any members of the school community.

All parents need to sign in the box below to show that they have read, understood and agree to the Acceptable Use Agreement.

Parent/carer's signature:			
Child's name:		Class:	