Online Safety Procedure

Church Gresley Infant and Nursery School

This procedure should be read in conjunction with the JTMAT Safeguarding Policy

Approved by:	LGB	**Date:**	29th September 2026
Last reviewed on:	03/9/26		
Next review due by:	September 2027		

Written by J Cripps and V Asquith

September 2026

Contents

1. Aims 2
2. Legislation and guidance 2
3. Roles and responsibilities 3
4. Educating pupils about online safety 5
5. Educating parents about online safety 5
6. Cyber-bullying 6
7. Mobile Technologies..... 6
8. Use of Video and Digital Images 6
9. Staff using work devices outside school 7
10. Social Media 7
11. How the school will respond to issues of misuse 8
12. Training 8
13. Filtering and Monitoring arrangements 9
14. Links with other policies 11

.....

1. Aims

Our school 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

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, misinformation, disinformation and conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

2. Legislation and guidance

This approach 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 headteachers and school staff

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.

Non-statutory guidance from the Department for Education on sharing nude and semi-nude images is available here and is used to support section 7 of this procedure.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this procedure and reviewing its effectiveness. They are also responsible for holding the Headteacher to account for its implementation.

The Designated Safeguarding Lead (DSL) will provide data to the Governing Body as part of the Headteacher's report on a half termly basis. Online Safety discussions will take place between the DSL and Safeguarding Link Governor.

All governors will:

- Ensure that they have read and understand this procedure
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this procedure, and that it is being implemented consistently throughout the school. They and the Deputy Headteacher are also responsible for ensuring the correct procedures are followed in the event of a serious online safety allegation being made against a member of staff (please see Appendix A 'Responding to an Online Safety Concern')

The Headteacher will:

- Ensure that there is a system in place to allow for online safety monitoring
- Provide regular monitoring reports to the governing body
- Establish and review the school online safety procedures and documents
- Ensure all staff know of the procedures that need to be followed in the event of an online safety incident taking place
- Provide training and advice for staff
- Ensure that they receive the online safety procedure for any alternative provision settings that the school pupils attend
- Liaise with the JTMAT technical staff and DSCB
- Receive reports of online safety incidents and create a log of incidents

3.3 The Designated Safeguarding Lead

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

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

- Ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the Headteacher, Senior IT Technician 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 procedure
- Ensuring that any incidents of cyber-bullying and online abuse are logged and dealt with appropriately in line with the school behaviour procedure

- Delivery of online safety information through Safeguarding CPD programme and Safeguarding updates
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 Technical Staff

Those with technical responsibilities are responsible for ensuring:

- Monitoring and maintaining 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
- 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 procedure
- Implementing this procedure consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet JTMAT-ICT-Security-Acceptable-Use-Policies.pdf 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 procedure.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.

The online safety lead will receive regular updates through attendance at external training events and network meetings and will review guidance documents as and when necessary.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this procedure
- Read and utilise the information available on the school website to promote Online Safety at home.
- Monitor their child's use of social media and ensure they are safe when using the internet.
- Monitor their child's mobile device and online activity, particularly in reference to online hoax material and online challenges.
- Use social media communications appropriately and positively, especially when making reference to the school or staff specifically, avoiding situations where negative or derogatory comments are posted in the public domain.

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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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 procedure, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use: JTMAT-ICT-Security-Acceptable-Use-Policies.pdf

4. Educating pupils and online safety

In EYFS, children will learn about living in a technological world and will build listening skills, curiosity, creativity and problem solving, through a variety of computing activities. They will be able to explore technology in many ways, including through use of ipads, laptops, the interactive whiteboard, taking photographs and using Beebots. They will be introduced to relevant vocabulary and will be familiar with a range of technologies providing a strong basis for Key Stage One.

At Key Stage One, pupils will be taught to:

- understand what algorithms are, how they are implemented as programs on digital devices, and that programs execute by following precise and unambiguous instructions
- create and debug simple programs
- use logical reasoning to predict the behaviour of simple programs
- use technology purposefully to create, organise, store, manipulate and retrieve digital content
- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. This curriculum should be broad, relevant and provide progression, with opportunity for creative activities. Pupils should be taught in all lessons to be critically aware of the materials/content they access on line and be guided to validate accuracy of information. Online safety messages will be reinforced at the start of each computing lesson.

Pupils should be taught to adopt safe and responsible use both within and outside school.

Staff should act as good role models in their use of digital technologies, the internet and mobile devices.

All teachers are responsible for ensuring that teaching and delivery is adapted to meet the needs of their students, including those with SEND and those who are vulnerable.

The school may also use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

Many parents and carers will only have a limited understanding of online safety risks and issues. They may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure how to respond.

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This procedure will also be shared with parents via our website, with reference to relevant websites including swgfl.org.uk ,Openview Education, www.saferinternet.org.uk, www.childnet.com/parents-and-carers

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a member of the Safeguarding Team.

Concerns or queries about this procedure can be raised with any member of staff or the Head of School.

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 school behaviour procedure.)

6.2 Preventing and addressing cyber-bullying

Whilst, due to the age of our pupils, incidents of cyber bullying may be rare, to help prevent it, 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. This will be done through the use of age appropriate books, eg 'Webster's Manners', 'Troll Stinks'

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

The school also has information links available on the website to support parents and carers with Online Safety.

7. Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include:, smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilizing the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The school allows:

	School Devices			Personal devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	No	Yes	Yes- but not in areas where pupils are
Full Network Access	Yes	Yes	Yes	No	No	No
Internet Access					Yes	Yes

8. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate our children at an appropriate level for their age, as part of our internet safety teaching, and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Pupil's work can only be published with the permission of the parents and carers of that pupil.

8.1 Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, to conduct school business, or on school systems (e.g. by remote access).

- Users must immediately report, to the nominated person – in accordance with the school procedure, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature or otherwise contravenes the rules defined by this policy and must neither respond to any such communication, or record or copy it in any way.

- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school website.

9. Staff using work devices outside 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, as set out in JTMAT-ICT-Security-Acceptable-Use-Policies.pdf

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 Senior IT Technician.

Work devices must be used solely for work activities. Staff should be aware that all laptops and PCs are covered by our monitoring software.

10. Social Media

Church Gresley Infant and Nursery School has a Facebook Page and an Instagram account. These are identifiable as:

Facebook: **Church Gresley Infants**

Instagram: **churchgresleyinfants**

We acknowledge that some individual staff and departments may choose to use social media as a way of communicating with our wider community in their professional capacity. Staff who do this must ensure that their activity and interactions online meet the expectations of the JTMAT Staff Code of Conduct. Personal activity on social media is also covered in the JTMAT Staff Code of Conduct.

Under no circumstances are any members of our school community permitted to create imitation or impersonation accounts online. Such accounts created will be reported via the Report Harmful Content button on our school website and if such accounts contain any illegal information they will be reported to the Police.

Our social media platforms are not formal methods of communication between stakeholders and school. We ask that you contact the School Office directly to raise any concerns.

11. How the school will respond to issues of misuse

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.

It is expected that all members of the school community will be responsible users of Computing technology, who understand and follow this procedure. However, there may be times when infringements of the procedure could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Please refer to the flowchart in Appendix A for the appropriate response.

12. 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).

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:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - 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 the risks up
- 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 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.

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.

15. Filtering and Monitoring arrangements

15.1 Roles and Responsibilities

All Staff

All staff are responsible for ensuring they are safe online and comply with the JTMAT Acceptable User Policy. All staff are responsible for reporting any concerns about online safety.

Student online safety concerns are reported via MyConcern.

Staff online safety concerns are reported to the Headteacher and then logged appropriately.

Concerns about filters, including allowing access and blocking access must be logged with the Headteacher

Teaching Staff

Teaching staff using computer facilities around school are responsible for ensuring students are using the IT equipment and online facilities in a safe way and for physically monitoring the use of IT equipment.

Senior Leadership Team

The SLT are responsible for ensuring that IT provision in school is adequately meeting the needs of staff and students, balancing the need for effective safeguarding, filtering and monitoring with providing high quality teaching and learning.

Governing Body

The Governing Body are responsible for ensuring that the school meet the requirements of KCSIE 2026 and the published safety standards.

Designated Safeguarding Lead

The DSL has the lead responsibility for Online safety, filtering and monitoring.

Deputy Designated Safeguarding Leads

The DDSLs will support the day-to-day management of online safety referrals.

IT Support Staff

Are responsible for the day-to-day maintenance of the IT infrastructure and filtering in place on the school network.

Are responsible for running the filtering checks and sharing the reports with the DSL.

Are responsible for running a termly report on updated (added/removed) filters with reasons and sharing this with the DSL.

15.2 Filtering

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this procedure are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their

online safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

• There will be regular reviews and audits of the safety and security of school technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

The “master/administrator” passwords for the school systems, used by the Network Manager (or other person) are implemented centrally for all schools who are part of the MAT network.

• The technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs). This is managed for CGINS via Endpoint Manager on the MAT network.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband filtering provider, Netsweeper by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.

• Staff and pupil filtering is implemented through proxy ports currently. There are different filtering levels for staff and students.

• Appropriate security measures are in to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software through the MAT network.

• An agreed procedure, in the JTMAT ICT Acceptable Use Policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

• An agreed procedure, in the JTMAT ICT Acceptable Use Policy is in place regarding the extent of personal use that users (staff / pupils) and their family members are allowed on school devices that may be used out of school.

• An agreed procedure, in the JTMAT ICT Acceptable Use Policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.

• An agreed procedure, within the JTMAT ICT Acceptable Use policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

15.2 Monitoring

The school’s IT system is monitored by Securus. This is a paid service that tracks keystrokes across all IT platforms including Microsoft Office, Online search engines and all other interfaces. The captures are automatically generated by the system and the DSL then reviews these captures by staff and students and they are then assigned a grading 1-5, with 5 being most significant.

The DSL and Deputies log behaviour and safeguarding issues related to online safety. Online safety incidents are reported via MyConcern. All staff are responsible for monitoring online safety when using IT facilities in school and reporting student issues via MyConcern.

The Deputy Head has undertaken training to enable her to support the investigation of online safety incidents.

If the monitoring system flags harmful material that is not being filtered the DSL and DDSL will log this with the IT Support Staff to ensure access to these sites are removed.

All staff have a responsibility to log any unfiltered websites with the IT Support Staff where they believe access to this site would pose a risk to children. This must be logged by contacting the IT Help Desk via Email.

The IT Support staff will then record the action taken and keep a record of this.

Each term the DSL will review the filtering lists in school. The DSL can also run a filtering test as part of the review to ensure compliance with recommended safety standards.

In addition to the external monitoring, the IT Support Staff are able to track login information within school and externally, this can be done when school login information is used on school and personal devices.

This procedure will be reviewed annually by the DSL. At every review, the procedure will be shared with the governing board and staff.

16. Links with other policies

This Online Safety Procedure is linked to our:

- JTMAT Child protection and safeguarding policy
- CGINS Approach to Safeguarding
- JTMAT Staff Code of Conduct
- JTMAT Data protection policy and privacy notices
- JTMAT Comments, Compliments and Complaints procedure
- ICT Security- Acceptable Use Policy