LEICESTER GRAMMAR JUNIOR SCHOOL

ICT Acceptable Use and Online Safety (E-Safety) Policy

This is a safeguarding policy. It should be read in conjunction with other policies: IT & Computing
Curriculum, Safeguarding, Anti-bullying, Use of Pupil Images, Use of Mobile Phones and Cameras. It should also be read in line with the Prevent Duty.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

This is a whole school policy and also applies to EYFS.

The school will monitor the impact of the policy using logs of reported incidents, by monitoring logs of internet activity and filtering, and through discussion with stakeholders

1. INTRODUCTION

This online safety policy outlines the commitment of Leicester Grammar Junior School to safeguard member of our school community on line in accordance with statutory guidance and best practice.

Leicester Grammar Junior School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The LGJS Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- allocates responsibilities for the delivery of the policy.
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours.
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- describes how the school will help prepare learners to be safe and responsible users of online technologies.

- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- is supplemented by a series of related acceptable use agreements.
- is made available to staff at induction.
- is published on the school website.

The school will monitor the impact of the policy using:

- logs of reported incidents
- Software and firewalls to monitor internet activity
- surveys/questionnaires of the school community

2. ROLES AND RESPONSIBILITIES

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline specific online safety roles and responsibilities:

2.1 Trustees

Trustees are responsible for the approval of this policy and for reviewing the effectiveness. They can use questions from the UKCIS Document '*Online Safety in Schools and College – questions from the governing body'.*

The review will be carried out by the safeguarding trustee who will meet regularly with the online safety lead (also the DSL).

The Safeguarding and Well-being Sub Committee will receive termly reports and information about online safety incidents.

2.2 Headteacher and Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL).

The Headteacher and Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority/MAT/other relevant body* disciplinary procedures)

The Headteacher and Senior Leaders are responsible for ensuring that the DSL, technical staff and other relevant staff receive suitable training to enable them to carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive monitoring reports from the DSL

2.3 Online Safety Lead and Designated Safeguarding Lead (DSL)

In their role as online safety lead, the DSL will take day to day responsibility for online safety, will be trained annually in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

They will:

- have a leading role in establishing and reviewing the school online safety policies and procedures
- promote an awareness of and commitment to online safety education/awareness raising across the school and beyond
- ensure that all staff are aware of the procedures to be followed in the event of an online safety incident taking place
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure there is appropriate training and advice for staff/trustees/parents/carers/pupils
- liaise with the Local Authority when necessary
- liaise with school technical staff
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- meet termly with the Safeguarding and Well-being Sub Committee to discuss current issues and to review procedures.
- report to the leadership team
- attend Safeguarding and Well-being sub-committee meetings with safeguarding trustees

2.4 Curriculum Leads

Curriculum Leads will work with the Online Safety Lead (DSL) to develop a planned and coordinated online safety education programme based on Project EVOLVE.

This will be provided through:

- computing lessons
- Jigsaw PHSE and RSE programmes

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Antibullying week.

2.5 Technical Staff

Those staff with technical responsibilities are responsible for ensuring:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- that the technical infrastructure is not open to misuse or malicious attack and that Leicester Grammar Junior School meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- to monitor Impero alerts and pass to the DSL
- to monitor use of the network in order to report misuse to the Headteacher for investigation • that monitoring software/systems are implemented.

•

2.6 Teaching and Support Staff

Are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current online safety policy and practices
- they understand that online safety is a core part of safeguarding.
- they have read and understood the staff code of conduct and the *Guidance for safer working practice for those working with children and young people in education settings February 2022* which includes sections about acceptable use of IT.
- they report any suspected misuse or problem to the DSL for investigation/action in line with school safeguarding procedures
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum
- pupils understand and follow this policy and the acceptable use policies
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc.

in lessons and other school activities and implement current policies with regard to these devices

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found during internet searches
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

2.7 Pupils

Pupils are responsible for using Leicester Grammar Junior School digital technology systems in accordance with the pupil use agreement (see appendix).

Pupils should:

- understand the importance of reporting abuse, misuse or access to inappropriate materials and be taught how to do so
- be expected to know and understand policies on the use of mobile devices and digital cameras, including the taking/use of images
- be taught to how to recognise and respond to online-bullying
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the online safety policy covers their actions out of school, if related to their membership of the school
  are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety

2.8 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use online services and devices in an appropriate way. Leicester Grammar Junior School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website, social media and information about national/local online safety campaigns/literature.

Parents and carers will be encouraged to support the school in

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices

3. FILTERING AND MONITORING

3.1 What is filtering and monitoring?

Filtering and monitoring systems are used to keep pupils safe when using the school's IT system.

Filtering systems: block access to harmful sites and content.

Monitoring systems: identify when a user accesses or searches for certain types of harmful content on school and college devices (it doesn't stop someone accessing it). School is then alerted to any concerning content to intervene and respond.

While filtering and monitoring reduces the risk of harm to pupils, no filtering and monitoring system is 100% effective and therefore these systems are used alongside additional safeguarding systems and procedures.

The IT Manager works alongside the DSLs within the LGS Trust to:

- Provide and implement a filtering and monitoring system
- Document what is blocked or allowed and why
- Review the effectiveness of the provision
- Ensure that incidents are urgently identified and acted upon with outcomes recorded
- Ensure staff understand their role in keeping children safe
- Reviewing the filtering and monitoring systems annually

4. EDUCATION

4.1 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

The following documents are referred to when planning the online safety curriculum:

DfE Teaching Online Safety in Schools
Education for a Connected Word Framework
SWGfL Project Evolve – online safety curriculum programme and resources

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression and will be provided in the following ways:

- Through a planned and regularly revisited online safety curriculum, provided as part of Computing, PSHE and other lessons as appropriate.
- A programme of assemblies and classroom activities will reinforce key online safety messages.
- Pupils will be taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will be supported in building resilience to radicalisation by providing a safe and supportive environment for the discussion of controversial issues and by helping them understand how they can influence and participate in decision-making.
- Pupils will be helped to understand the need for the pupil acceptable use agreement and will be encouraged to adopt safe and responsible use both within and outside school. Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- If pupils are allowed to freely search the internet, staff should move about and be vigilant in monitoring the content of the websites.

4.2 Parents/carers

Some parents/carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of online behaviours. Parents 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.

Awareness will be raised through the school website, through information evenings, and through participation in high profile events such as Safer Internet Day.

4.3 Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Online safety training will be provided during safeguarding training, at safeguarding update meetings and as part of the induction process. In addition, the DSL will regularly review guidance documents released by relevant organisations.

5. PROVIDING REMOTE EDUCATION

LGJS recognises that attendance is essential for pupils to get the most out of their school experience, including for their attainment, wellbeing, and wider life chances. At LGJS remote education should only ever be considered as a last resort where a decision has already been made that attendance at school is not possible, but will be provided to ensure pupils are able to continue learning.

Each case is different and will be provision will be considered on an individual basis.

The DfE document 'Providing remote education' will be used to plan and deliver remote learning alongside advice from local partners (for example inclusion services and hospital school)

Where remote education is taking place, LGJS will maintain professional practice and when communicating online with parents, carers and children:

- staff will communicate within school hours as much as possible (or hours agreed with the school or college to suit the needs of staff)
- communication will be through the school or college channels approved by the senior leadership team
- staff will use school or college email accounts (not personal ones)
- staff will use school devices
- staff will not share personal information
- there will be guidelines to ensure parents and carers are clear when and how they can communicate with school staff
- staff will ensure login details and passwords are secure and children understand that they should not share this information with others. Ideally communication should be via Microsoft Teams. This can be via a pupil email (Year 3 upwards) or via a parent email.

If teachers are teaching children from their own homes or any other shared space (for example, if school access is restricted and teachers and children cannot attend in person) they should aim to find a quiet space to communicate with children, parents or carers. If using video communication software, they should use a neutral or plain background.

6. ILLEGAL INCIDENTS

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart below and report immediately to the police.

7. MISUSE: STATEMENT OF POLICY

Leicester Grammar Junior School will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB. If the school discovers that a child is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The school will impose a range of sanctions to any child who misuses technology to bully, harass to abuse another pupil in line with the anti-bullying policy.

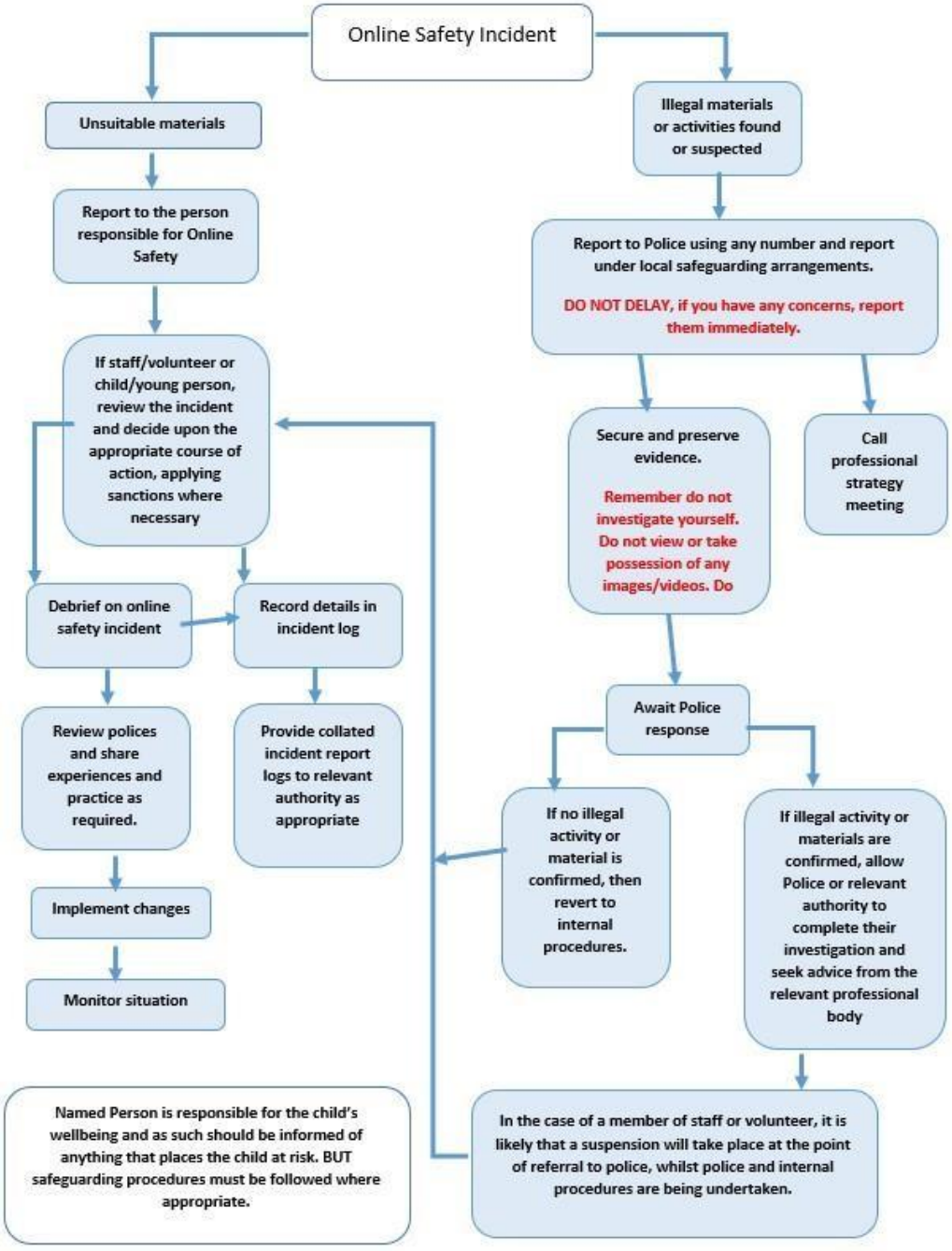
8. PUPIL PERSONAL DEVICES

Pupils are not permitted to bring to school a mobile phone or any other device allowing access to the internet or which can be used to record and store images. This includes watches. In exceptional circumstances, for example, for pupils travelling on the school bus permission will be granted on a case-by-case basis and at the discretion of the headteacher.

During the school day the phone will be stored with the class teacher or office staff and will be returned as agreed with the headteacher or when the pupil boards a bus.

9. USEFUL RESOURCES

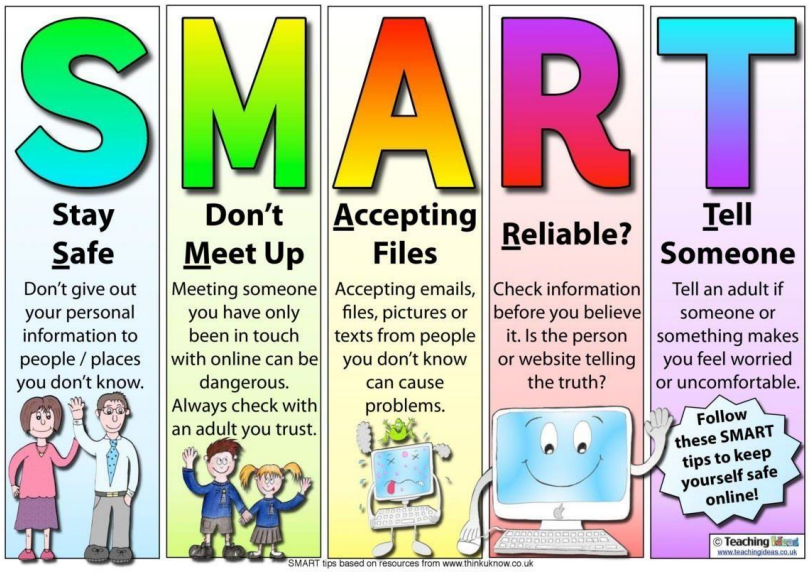
- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Child Expoitation Online Protection (CEOP) (www.thinkuknow.co.uk)
- Childnet International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)
- Online safety for educators, parents and carers (http://www.digizen.org)


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Acceptable Use Agreement (KS2)

Name of pupil:

- I will ask a grown up before using a device and ask for help if I cannot work the device
- I will only use activities that a grown-up has allowed me to use
- I will tell a grown up if I see something that upsets me on the screen
- I know that passwords keep information safe, therefore I will not share any passwords
- I will never use technology, including my school email or Teams chat, to send messages which could upset another person
- I will only open, edit and delete my own files
- I will never give any personal details to strangers I meet online
- I will follow the SMART rules:



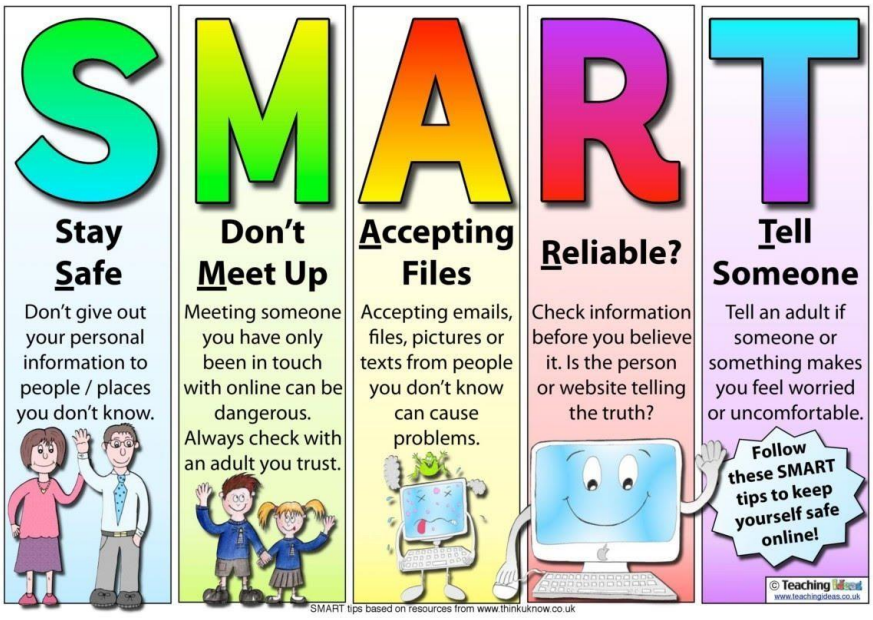
Signed (pupil):	Date:

Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet and will make sure my child understand these.	
Signed (parent/carer):	Date:

Acceptable Use Agreement (KS1)

Name of pupil:

- I will ask a grown up before using a device and ask for help if I cannot work the device
- I will only use activities that a grown-up has allowed me to use
- I will tell a grown up if I see something that upsets me on the screen
- I know that passwords keep information safe, therefore I will not share any passwords
- I will follow the SMART rules:



Signed (pupil):	Date:
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet and will make sure my child understand these.	
Signed (parent/carer):	Date:

Acceptable Use Agreement (EYFS)	
Name of pupil:	
• I will ask a grown up before using a device and ask for help if I cannot work the device • I will only use activities that a grown-up has allowed me to use • I will tell a grown up if I see something that upsets me on the screen	
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet. I will take time to discuss this agreement with my child and will make sure my child understand the points listed above.	
Signed (parent/carer):	Date: