Lancaster Royal Grammar School
Digital Safety Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Schedule for Development, Monitoring and Review

This Digital Safety Policy was approved by the *school Senior Leadership Team on:*	*November 2025*
The review of this policy by the Senior Leadership Team is, the next scheduled for:	*November 2026*
The implementation of this Digital Safety Policy will be monitored by: *James Hallsworth (Deputy Head: Pastoral – DSL) supported by David Rowe (Head of Boarding).*	
The Digital Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The *Safeguarding Trustee Committee* will receive a report on the implementation of the Digital Safety Policy at regular intervals.	

Digital Safety Policy

The school Digital 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 pupils in the digital world
- describes how the school will help prepare pupils 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.

Scope of the Digital Safety Policy

This Digital Safety Policy outlines the commitment of Lancaster Royal Grammar School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Digital Safety Policy applies to all members of the school community (including staff, pupils, Trustees, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed), and when connected with the membership of the school in line with the Behaviour of Pupils Policy.

Lancaster Royal Grammar 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.

Policy development, monitoring and review

This Digital Safety Policy has been developed by the Senior Leadership Team and the Digital Safety Group.
The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *filtering and monitoring logs*

- *internal monitoring data for network activity*
- *surveys/questionnaires of: pupils; parents and carers; staff.*

Policy and Leadership

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 the online safety roles and responsibilities of individuals and groups within the school.

Headteacher and senior leaders

- 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 is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff 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/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.
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead through the 'Safeguarding and Pupils' standing item at SLT meetings.
- The headteacher/senior leaders will work with the responsible Trustee, the Designated Safeguarding Lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Trustees

Trustees have delegated the review of this policy to the SLT, but are responsible for reviewing the effectiveness of the policy through the Safeguarding Sub-Committee.
This review will be carried out by the Safeguarding Sub-Committee whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Trustee to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Digital Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, the Network Manager and Deputy Network Manager and involve the responsible Trustee) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant Trustees group/meeting
- Receiving (at least) basic cyber-security training to enable the Trustees to check that the school meets the DfE Cyber-Security Standards
- membership of the school Online Safety Group

Designated Safety Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the Online Safety Trustee to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant trustee body meetings/groups

- report regularly to headteacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Leads (Pastoral Heads)

The Online Safety Leads will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL),
- receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- 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
- provide (or identify sources of) training and advice for staff/Trustees/parents/carers/pupils
- liaise with technical staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by pupils) with regard to the areas defined In Keeping Children Safe in Education: content; contact; conduct; commerce
- the production/review/monitoring of the school Digital Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of pupils to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Curriculum Leads (Curriculum Forum)

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme
This will be provided through:

- a discrete programme
- PHSE (Values) and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- will assist the DSL/OSL by mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage

Digital Safety Group

The Digital Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and monitoring the Digital Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to senior leaders.

The Online Safety Group has the following members:

- Designated Safeguarding Lead – standing member
- Pupil Digital Safety Ambassadors – standing members
- Online Safety Trustee – standing member
- Pastoral Heads – by invitation
- senior leaders – by invitation
- technical staff – by invitation
- teacher and support staff members – by invitation
- parents/carers representative – by invitation

Members of the Digital Safety Group will assist the DSL/OSLs with:

- the production/review/monitoring of the school Digital Safety Policy/documents
- the production/review/monitoring of the school filtering policy and requests for filtering changes
- reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- being a pupil forum to discuss emerging trends and the school online safety provision
- leading digital and online safety initiatives including planning and delivering online safety week messages

Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Digital Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with pupils, parents and carers and others should be on a professional level *and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements*
- they immediately report any suspected misuse or problem to **David Rowe (Head of Boarding)** for investigation/action, in line with the school safeguarding procedures
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Digital Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned pupils are 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*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is 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.
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the pupils in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Network Manager and Commissioned Services

If the school has a technology service provided by an outside contractor, it is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Digital Safety Policy and procedures.

The Network Manager is responsible for ensuring that:

- they are aware of and follow the school Digital Safety Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority or other relevant body
- there is clear, safe, and managed control of user access to networks and devices

- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to **Kevin Gilpin (Network Manager)** for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Pupils

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Digital Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Digital Safety Policy covers their actions out of school, if related to their membership of the school

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Digital Safety Policy on the school website
- providing them with a copy of the pupils' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Reporting and Responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Leads and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident must be escalated through the agreed school safeguarding procedures, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse

        - Fraud and extortion
        - Harassment/stalking
        - Child Sexual Abuse Material (CSAM)
        - Child Sexual Exploitation Grooming
        - Extreme Pornography
        - Sale of illegal materials/substances
        - Cyber or hacking offences under the Computer Misuse Act
        - Copyright theft or piracy
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Trustees
- where AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process - this is vital to protect individuals if accusations are subsequently reported
    - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected - use the same device for the duration of the procedure
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern - it may also be necessary to record and store screenshots of the content on the machine being used for investigation
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not - if it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged using the school's CPOMS system
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - the Pastoral Heads for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
    - staff, through regular briefings
    - pupils, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - Trustees, through regular safeguarding updates
    - local authority/external agencies, as relevant

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. The actions of staff will be dealt with under the terms of the Low Level Concerns Policy and the Disciplinary Procedures for Teachers and Support Staff

Online Safety Education Programme

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 should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupil need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services)
- pupils should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- staff should 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 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
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites / tools (including AI systems) the pupils visit
- it is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes

Filtering & Monitoring

- the school filtering and monitoring provision is agreed by senior leaders, Trustees and the IT Department and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours
- day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility
- the filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a Trustee with the involvement of the IT Department
- checks on the filtering and monitoring system are carried out by the IT Department with the involvement of a senior leader, the Designated Safeguarding Lead and a Trustee, in particular when a safeguarding risk is identified, there is a change in working practice

Filtering

- a member of the SLT and a Trustee, are responsible for ensuring these standards are met - roles and responsibilities of staff and third parties, for example, in-house or third-party IT support are clearly defined

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office - content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective. These are acted upon in a timely manner, within clearly established procedures
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon
- there are regular checks of the effectiveness of the filtering systems - checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision - the DSL and Trustee are involved in the process and aware of the findings
- devices that are provided by the school have school-based filtering applied irrespective of their location
- the school will (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/pupils, etc.)
- the school has a mobile device (phone) policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice
- If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance.

The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users:

- the school monitors all network use across all its devices and services
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that monitoring is in place
- there are effective protocols in place to report abuse/misuse - there is a clear process for prioritising response to alerts that require rapid safeguarding intervention
- management of serious safeguarding alerts is consistent with safeguarding policy and practice
- the monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours - the review should be conducted by members of the senior leadership team, the designated safeguarding lead, and technical staff - it will also involve the responsible Trustee - the results of the review will be recorded and reported as relevant
- devices that are provided by the school have school-based monitoring applied irrespective of their location
- monitoring enables alerts to be matched to users and devices.
- where AI –supported monitoring is used, the purpose and scope of this is clearly communicated

Social Media & Website

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.

- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for pupils, parents/carers

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- they act as positive role models in their use of social media

Pupils should ensure that:

- they do not create or contribute to unofficial social media accounts linked to the membership of the school

When official school social media accounts are established, there should be:

- a process for approval by the Marketing Manager
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse

The school website is managed/hosted by (Juniper Education). The school ensures that Digital Safety Policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.
Where pupil work, images or videos are published, their identities are protected, and full names are not published.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and 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 users about these risks and will implement policies to reduce the likelihood of the potential for harm (select/delete as appropriate):

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies
- when using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those pupils whose images must not be taken/published - those images should only be taken on school devices - the personal devices of staff should not be used for such purposes
- 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, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that pupils are appropriately dressed
- 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 Digital Safety Policy
- pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media - permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy

Outcomes

The impact of the Digital Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Trustees
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

LRGS Student Mobile Phone and Digital Device Acceptable Use Agreement

The Policy In Brief:

1. We expect you to be **kind and thoughtful** when using technology.

2. The school have a **balanced approach**: taking advantage of benefits of technology but having rules to protect pupils & staff and promote good behaviour.

3. Year 7-11 pupils are **not allowed to use their mobile phones or digital devices in school – they must be turned off and in your bag.** Your teacher may allow you to use your phone in lessons, it's their decision not yours.

4. Sixth Form pupils can use their devices **before 8.45am**, and at **break and lunch**, and whenever they are in one of the Sixth Form Cafés, however your phone will be confiscated if you:

    a. Use it around school outside permitted times e.g. in between lessons

    b. Walk around school using it, including with headphones or buds, at any time;

    c. Use your device in a device free zone (like the Grab & Go or Dining Hall);

    d. Photograph, film, or record a pupil or member of staff;

    e. Use your device in a way which causes issues or makes people feel uncomfortable.

5. If we confiscate your phone or device, **you get it back then next day** – you should go to one of the school offices and ring someone from home to **let them know you don't have your phone** – if this causes a real issue you should speak to someone in the pastoral team.

6. The school will take action if you post upsetting things about people at school online.

7. 'Unofficial' LRGS accounts and form/class groups can become spaces with harmful, upsetting or unkind content – please think **very carefully** before setting them up or contributing.

8. **The school network is monitored**. We try to give you some privacy, but if your username is flagged by the system we will have to look into what you've been doing. We also look at pupil email accounts if we think you've been using the system inappropriately.

The Policy In Full:

School Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe and appropriate internet access, however it is the school's desire to balance the benefits of technology with attitudes and rules conducive to good behaviour, mental health and social wellbeing.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

The access to and use of the internet, school network and digital devices by students is on condition that they accept and uphold the following statements about their behaviour and use:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the school filter access to the internet and block inappropriate, harmful or illegal content.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of danger presented by people that I do not know, when I am communicating on-line.
- I am aware that people with extreme views may use the internet to try to involve me in illegal or terrorist activity.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that the school have a differentiated approach towards the rights and permissions of users and:

- I understand that this means that the rules relating to use are not the same for all students; differentiated rules will ensure all users use technology in a safe and appropriate way.

I understand that the school's ICT systems are primarily intended for educational use and:

- I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work and that it is acknowledged and referenced appropriately.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that the school's behaviour of pupils, anti-bullying, and pupil relationships policies may apply to my online actions out of school.
- I understand that the school provide platforms for groups and teams to communicate digitally and as such do not endorse any 'unofficial' groups or accounts. I understand that labelling something 'unofficial' does not remove its connection to the school. I understand that I do not have permission to create online groups linked to the membership of the school without permission from a member of staff.
- I understand that creating parody, fake or unofficial accounts linked to LRGS or members of its community is potentially harmful or upsetting and the school may take action against those who do so.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, exclusions, contact with parents and, in the event of illegal activities, involvement of the police.

I understand that the school operate a 'Bring Your Own Device' policy which means I may bring my own technology to school and use it under the following terms:

- In terms of this policy 'devices' are defined as an electronic technology which may have internet connectivity, including but not limited to: phones, tablets, computers, smart watches, gaming devices and other similar devices.
- All users must adhere to this policy regardless of who owns the device being used.
- The school has a set of clear expectations and responsibilities for all users, detailed in this policy.
- The school adheres to the Data Protection Act principles.

- All users are provided with and must act within this Acceptable Use Policy.
- Where possible these devices will be covered by the school's normal filtering and monitoring systems, while connected to the school's network.
- The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. The school permits users to bringing their own technologies to school in order to provide a greater freedom of choice and usability. However, the school has a differentiated approach to the use of these devices during the school day as follows:
    - **Pupils in Year 7 to 11:** are **not** permitted to use their devices during the school day, nor on the school site, **their devices must be switched off and in their bags at these points**. A teacher may give permission for these students to use their devices in lessons for a purpose which supports their learning.
    - **Sixth Formers:** are only permitted to use their mobile devices **before 8.45am**, and **during break and lunchtime**, and with the permission of their teacher in lessons in order to support their learning. The following rules apply at **all points** in the school day:
        - The use of a mobile device is prohibited when travelling around the site and crossing roads – this includes using headphones or buds – because we need you to pay full attention to your surroundings.
        - The use of a mobile device is prohibited in toilets and changing rooms.
        - The use of a mobile device is prohibited in the Dining Hall and Grab and Go which are designated device free zones.
        - At no point must any member of the school community use their device in a way which disrupts teaching and learning, brings the school into disrepute, or adversely affects the safety and wellbeing of members of the school community.
        - The use of mobile devices must not contravene the school's behaviour of pupils, anti-bullying, pupil relationships policies or this Acceptable Use Policy.
        - Personal mobile devices must not be used for the taking of photographs, video or recordings of members of the school community. Nor will these features be used by students for other purposes on the school site without the permission of a member of staff.
    - Sixth Formers may use their phones in the Sixth Form Cafés. They are not allowed in the downstairs study space but can be used for work purposes in the upstairs study space to support their learning.

I understand and accept the consequences for students who misuse technology in school and that:

- The devices of students who fail to maintain these principles will be **confiscated** by a member of staff.
- The school operate a **next day return on confiscated devices**; confiscated devices may be collected the following morning from City View.
- Exceptions will be made for students with Health Care Plans who can pick up their phone at the end of the school day. Students who've had their device confiscated and need to contact their parents or carers may do this from any of the school receptions.
- In **exceptional circumstances**, a senior member of the pastoral team (such as a Head of Year) may decide that the confiscated phone may be returned to a student in order to safeguard them on their journey home. An equivalent consequence will be agreed.
- Students who have had their phone confiscated on Friday may choose to collect their phone from the City View reception at the end of school on Friday on the understanding that it is returned on Monday morning before registration, it can be collected on the following Tuesday.
- Before a confiscated phone is returned the student will have to demonstrate their understanding of the rules. In some instances, parents may be asked to collect the device and the student may forfeit the right to use their phone in school.
- Mobile devices are allowed in school on the understanding that they are the responsibility of the individual. The school can take no liability for their loss or damage. If a member of staff confiscates a device, they must take measures to protect the student's device and ensure its safe return at an appropriate point.
- That the school will report illegal activity to the Police.