Ludgrove School

Online Safety / ICT Policy

Updated: September 2025

Summary Policy Statement

At Ludgrove School (Ludgrove), ICT is an integral part of the day-to-day life and has an impact on every child and staff member. We aim for our children to be responsible and effective users of technology and they are provided with opportunities to use ICT in their academic and extra-curricular life at School. We have robust systems in place to keep our children safe whilst using technology as a teaching and learning tool, beyond this, all members of the School Community are educated in avoiding the potential dangers associated with online lives outside of the school.

1. Policy Statement

1.1. Ludgrove School recognises that ICT and the Internet are integral tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to collaborate and share ideas can benefit all members of the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it responsibly, appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

1.2. Online safety covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings.

1.3. There is a 'duty of care' for any person working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

1.4. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures. (See Anti-bullying policy)

1.5. At Ludgrove school, we recognise the transformative potential of Artificial Intelligence (AI) in enhancing educational experiences and outcomes. Our ICT Policy is designed to ensure the responsible and ethical integration of AUI technologies within our curriculum, fostering a learning environment that is innovative, secure, and inclusive. Please refer to our AI Use Policy for more information regarding the use of AI at Ludgrove School.

2. Roles and Responsibilities

2.1. **Governors**

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety also falls within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include:

- ensure an online safety policy is in place, reviewed every year and is available to all stakeholders.
- ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- ensure that procedures for the safe use of ICT and the Internet are in place and adhered to; and
- hold the headmaster and staff accountable for online safety.

2.2. **Headmaster and SLT**

The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the online safety co-ordinator. Any complaint about staff misuse must be referred to the online safety coordinator at the school or, in the case of a serious complaint, to the Headmaster, to ensure:

- access to induction and training in online safety practices for all users.
- appropriate action is taken in all cases of misuse.
- Internet filtering methods are appropriate, effective, and reasonable.
- staff or external providers who operate monitoring procedures be supervised by a named member of SLT.
- pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- the school works in partnership with the DFE and the Internet Service Provider and school ICT Manager to ensure systems to protect students are reviewed and improved;
- the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- the Senior Leadership Team will receive monitoring reports from the online safety co-ordinator.

2.3. **Online safety coordinator:**

- Leads E-safety meetings.
- Work in partnership with the DFE and school Network Manager to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.
- Receives reports of e-safety incidents and creates a log of incidents to inform future online safety developments,
- Reports to Senior Leadership Team.
- Liaise with the nominated member of the governing body and/or headmaster to provide an annual report on online safety.

2.4. **Network Manager / Technical Staff:**

The Network Manager is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
- 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 its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the headmaster; online safety coordinator for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies; and
- Provide reports to governors on the above.

3. Communicating School Policy

This policy is available for staff online in the Shared Resource Library (CRL) and via the school website for pupils and parents. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed

around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

4. Making use of ICT and the Internet in school

The Internet is used in school to raise educational standards, aware of the online/digital environment to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education, and business. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently and safely into a professional working environment when they leave school. Some of the benefits of using ICT and the Internet in schools are:

4.1. **For pupils:**

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people, and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos, and interactive media to enhance understanding; and
- Individualised access to learning.

4.2. **For staff:**

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

4.3. **For parents:**

- Communication between School and Home on issues related to the education of their children and issues faced by the challenges and potential dangers of the online world.
- The main forms of communication are via Email, Parent Portal, or text messaging.

5. Learning to Evaluate Internet Content

5.1. With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read and shown how to validate information before accepting it as accurate.
- Use age-appropriate tools to search for information online, and
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

5.2. The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils.
5.3. If a member of staff or pupils discover unsuitable sites, then the URL will be reported to the school online safety coordinator.
5.4. Any material found by members of the school community that is believed to be unlawful will be reported to the online safety coordinator.
5.5. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

6. Managing Information Systems

Ludgrove School is responsible for reviewing and managing the security of the computers and Internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers, and other external security threats. The Network Manager will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted and in accordance with our Data Protection Policy.
- Making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this.
- Files held on the school network will be regularly checked for viruses.
- The use of user logins, passwords, and Two-factor Authentication (2FA) to access the school network will be enforced.
- Portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.
- Compliant with existing Data Protection legislative requirements.
- Our firewall and web filter (WatchGuard and Securely) filters all internet traffic and blocks sites which are deemed to be inappropriate. Internet searches are filtered for profanities, spam, and any inappropriate content.
- Securly Software Actively monitors website titles, content, open applications and typed words for safeguarding, security, and behavioural misuse of the computers – taking screenshots and (optionally) blocking access as Network Manager sees fit; and
- Virus protection throughout the school is updated daily.
- Senso Software is used for classroom management of devices and relevant access is given to those teachers who need it.

For more information on data protection in school please refer to our Data Protection Policy.

7. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to. See Staff Handbook.

7.1. **School Email Accounts and Appropriate Use**

- All Prep School children have their own Exchange/Webmail account. Children have no access to any other email accounts in school. Student email addresses are constructed using their surname and the first letter of their surname. In cases where their surname exceeds the characters limit for Exchange an abbreviated version will be used and communicated to all relevant parties.

- Children do not have access to external web-based email accounts such as Hotmail, Google mail etc.
- Pupils must complete, sign, and understand the Pupil Usage Acceptance Agreement before using the School's ICT.
- Staff have an Exchange email account which is accessible via the school network, remote access or via Smartphone (iPhone or Android). Staff are allowed to access their own personal emails via the school network.

7.2. **Staff should be aware of the following when using email in school:**

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers for school related matters. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are always representing the school and should take this into account when entering any email communications.
- Staff must tell their Computing Head or a member of the senior leadership team if they receive any offensive, threatening, or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.

7.3. **Pupils should be aware of the following when using email in school,** and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use school-approved email accounts.
- Pupils should tell a member of staff if they receive any offensive, threatening, or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves; and
- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge. Pupils will be educated through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

7.4. **Published Content and the School Website**

7.4.1. Ludgrove School website is viewed as a tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up to date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

7.4.2. The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights, and privacy policies. No personal information on staff or pupils will be published (unless with express consent), and details for contacting the school will be for the school office only. For information on the school policy on use of children's photographs on the school website please refer to our Data Protection Policy and Photo Policy.

7.4.3. As a marketing tool, the school website is maintained by the Marketing team and third-party website specialists as they see fit.

7.5. **Parent Portal**

7.5.1. The Parent Portal gives parents access to information related to their child whilst at Ludgrove School.

7.5.2. Parents are provided with a unique Username and Password which provides access to the platform.

7.5.3. Via the Parent Portal, parents can access, progress reports, news - important documents, exam results (academic, music), electronic forms for events and travel, staff contact details, School calendar, their child's academic timetable and the Sports App Link.

8. Policy and Guidance of Safe Use of Children's Photographs and Work

8.1. Colour photographs and pupils work bring Ludgrove to life, showcase Ludgrove student's talents, and add interest to publications both online and in print that represent Ludgrove. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

8.2. On admission to the school parents/carers will be asked to sign an image consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school's policy on the use of photographs of children, including:

- How and when the photographs will be used.
- How long parents are consenting the use of the images for; and
- Refer to our privacy policy and Data Protection Policy.

8.3. A template of the consent form can be found at Annex C.

8.4. Photographs, videos or any other types of images of pupils must not be uploaded onto personal social media unless the pupil's family consent has been given. For example, if your child is friends with a pupil who appears in a picture alongside them, the parents' permission must be sought before uploading of pictures of the children on to social media.

8.5. Ludgrove School's digital camera/s or memory cards must not leave the school premises except for use on outings. Photos are printed in the setting by staff and images are then removed from the camera's memory.

9. Using photographs of individual children

9.1. The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

9.2. It is important that published images do not identify students or put them at risk of being identified. The school is careful to make sure that images published on the school website are difficult to reuse or manipulate through browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the parent's and school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications
  - on the school website
  - in newspapers as allowed by the school
  - in videos made by the school or in class for school projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child, unless express parental consent have been obtained. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of pupils such as school plays or sports days must be used for private, personal use only, and not shared on social media.
- Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them, or they are being asked to participate in.
- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will always wear identification, and will not have unsupervised access to the pupils.

9.3. For more information on safeguarding in school please refer to our school Child Protection and Safeguarding Children Policy.

10. Complaints of Misuse of Photographs or Video

10.1. Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our Complaints Policy and Procedure for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools Child Protection and Safeguarding Children Policy.

10.2. Cyberbullying and sexting by pupils will be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm and will be managed through our anti-bullying procedures (See our Anti-Bullying Policy) and Child Protection and Safeguarding Children Policy. Serious incidents may be managed in line with our Child Protection and Safeguarding Children Policy.

11. Training

11.1. **Pupils**

11.1.1. Many pupils own or have access to handheld devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community.

11.1.2. Prior to using ICT at Ludgrove School, pupils must complete a 'Rules of the Road' (User Agreement), which outlines the rules of using ICT at the School. This can be found in Annex B.

11.2. **Parents**

The school regularly provides parent workshops or relevant document to make parents aware of how their children can use ICT in a safe manner. In addition, sessions focus on strategies to extend this safeguarding beyond the school and into the family home.

11.3. **Teaching Staff**

All teaching staff receive online safety training on an annual basis. In addition, INSET sessions related to the latest online safety trends are held at different times of the year.

11.4. **Governors**

All Governors receive online safety training on an annual basis.

12. Messaging Services

12.1. **Staff**

12.1.1. Staff must exercise professional judgement when using messaging services such as WhatsApp on personal or school-issued devices. While WhatsApp may be used for operational communication between colleagues, it must not be used to communicate directly with pupils or parents under any circumstances. All communication with pupils and parents must take place through approved school channels (e.g., school email or designated communication platforms).

12.1.2. Staff must ensure that any group chats related to school matters are appropriate, limited to relevant staff members, and do not contain any sensitive or personal information about pupils or staff as this communication may be covered in the event of a Subject Access Request. The school reserves the right to review the use of messaging services on school devices to ensure compliance with safeguarding, data protection, and professional conduct policies.

12.2. **Pupils**

12.2.1. Pupils are not permitted to use messaging services (such as WhatsApp, iMessage, Snapchat, or similar platforms) on personal or school devices during the school day, unless explicitly authorised by a member of staff for educational purposes.

12.2.2. All digital communication between pupils and staff must take place through approved school channels, such as the school email system or designated learning platforms (e.g., Teams, Firefly), and must always be respectful and appropriate.

12.2.3. Pupils must not use messaging services to share inappropriate, offensive, or hurtful content. Cyberbullying, exclusion of others, or the spreading of rumours or personal information will be treated as a serious disciplinary matter in line with the school's Behaviour and Safeguarding Policies.

12.2.4. Pupils should be aware that digital communications, including group chats, may be monitored where there is a safeguarding concern. They are expected to report any inappropriate messages or behaviour to a trusted adult or member of staff.

12.2.5. The use of messaging services is a privilege and must reflect the school's values of kindness, respect, and responsibility. Misuse may result in the restriction or removal of digital access and further disciplinary action.

13. Social Networking, Social Media, and Personal Publishing

13.1. Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school as many of our pupils do not meet the minimum required age. There are various restrictions on the use of these sites in school that apply to staff.

13.2. All network users must use an appropriate password and always remember to log out after use. It is the responsibility of the user, and it is critical that staff do not allow children access to their own personal account.

13.3. This policy deals with social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways when they meet the required minimum age limit. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful, or defamatory. The school expects all staff and pupils to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

13.4. **Staff use of Social Media**

13.4.1. Staff should be professional, responsible, and respectful when using social media.

13.4.2. When using social media staff must be conscious at all times of the need to keep your personal and professional lives separate. Staff should not put themselves in a position where there is a conflict between their work for the school and their personal interests.

13.4.3. **Staff must not:**

a) engage in activities involving social media which could damage the reputation of the school, even indirectly.

b) represent their personal views as those of the school on any social media. Staff should write in the first person and use a personal email address.

c) discuss personal information about School pupils, staff members and other professionals they interact with as part of their job at the school on social media.

d) include the school's logos or other trademarks in any social media posting or in their profile on any social media.

e) use social media and the Internet in any way to harass, bully, unlawfully discriminate against, attack, insult, abuse, disparage or defame pupils, their family members, staff members, other professionals, other organisations, or the school as an institution; to make false or misleading statements; or to impersonate colleagues or third parties.

f) express opinions on behalf of the school via social media, unless expressly authorised to do so by the Marketing Department. Staff may be required to undergo training to get such authorisation.

g) edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the school.

h) identify themselves as employees of the school or service providers for the school in their personal web space (use of professional web space such as LinkedIn is up to the user's discretion, keeping in mind that anyone such as parents, students and colleagues can access your profile and you must always comply with this policy). This is to prevent information on these sites being linked with the school and to safeguard the privacy of staff members, particularly those involved in providing sensitive front-line services.

i) accept 'friend requests' from current pupils or recent leavers they receive in their personal social media accounts.

j) "Check in" or tag their photos/videos at the school (this includes but is not limited to Facebook, Instagram, Twitter, Pinterest).

k) use School email addresses and other official contact details for setting up personal social media accounts or to communicate through such media. The use of School email addresses to create or join a School sanctioned social media site is appropriate.

l) on leaving the service of the school, contact the school's current pupils by means of personal social media sites. Similarly, staff members must not contact current pupils from their former schools by means of personal social media unless they are family-related/close friends with parents. It is advised to maintain professional conduct while communicating with former students for work or personal reasons.

m) have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

n) have contact through any personal social media with any current pupils, whether from the school or any other school, unless it is for professional contact, or the pupils are family members.

13.4.4. **Staff must be:**

a) respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the Internet for anyone to see.

b) accurate, fair and transparent when creating or altering online sources of information on behalf of the school.

13.4.5. If staff are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your Department Head.

13.4.6. If staff see social media content that disparages or reflects poorly on the school, they should contact a member of Senior Leadership Team (SLT).

13.4.7. The school permits limited personal use of social media while at work. Staff members are expected to devote their contracted hours of work to their professional duties, and, in practice, personal use of the Internet or social media should not be used during contact time (for teachers and teacher assistants), should never involve unprofessional or inappropriate content and must always comply with this policy.

13.4.8. Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Be mindful of having colleagues as friends on social media as it may be difficult to maintain professional relationships, or it might be just embarrassing if too much personal information is known in the workplace.

13.4.9. Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and opt out of public listings on social networking sites to protect their own privacy.

13.4.10. Staff members can only use officially sanctioned School social media tools for communication on behalf of the school. Requests for this type of communication should go via the Marketing Department who have access to the relevant social media tools.

13.4.11. There must be a strong pedagogical or business reason for creating official School social network sites to communicate with pupils or others. Staff members must not create sites for trivial reasons which could expose the school to unwelcome publicity or the posting of unwelcome material or damage its reputation.

13.4.12. Official school sites must be created according to the requirements provided by the Marketing Department. Sites created must not breach the terms and conditions of social media service providers, particularly regarding minimum age requirements.

13.4.13. Staff members must always act in the best interests of children and young people when creating, participating in or contributing content to social media sites. We are responsible for the safeguarding and protection of children.

13.5. **Mobile Phones, Wearable and Personal Devices**

13.5.1. While mobile phones, wearable devices (such as smartwatches) and other personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices include:

- Increased vulnerability to cyber bullying.
- The potential to access inappropriate internet material.
- Distraction from learning.
- Being valuable items that could be stolen, damaged, or lost.
- Integrated cameras or recording functions, which can pose child protection, bullying, and data protection risks.

13.5.2. In their free time, we want boys to be out and about, having fun with their friends and making maximum use of our grounds and facilities. Therefore, no personal mobile phones, iPads, wearable devices (e.g., smartwatches), or other electronic gadgets are allowed at school. Only top-year boys may bring back iPods/iTouches, and these are to be used exclusively for playing music. International students are permitted to travel to the school with a mobile phone or personal device; however, upon entering the school building, these devices must be handed in to the front office for secure storage. Devices are not returned until the student departs for home.

13.6. **Staff Mobile Phones and Wearable Devices**

13.6.1. Staff must use mobile phones and wearable devices (e.g., smartwatches) responsibly and in line with the school's safeguarding and professional conduct policies. Personal use should be limited to break times and away from pupils, unless required for operational or emergency purposes. Visitors may only use such devices outside the building and not in front of children (Please see Data Protection Policy).

13.6.2. Mobile phones and wearable devices must not be used to photograph, record, or communicate with pupils under any circumstances. All pupil-related communication and documentation must be carried out using approved school devices and platforms.

13.6.3. Staff should ensure mobile phones and wearable devices are kept on silent or non-intrusive modes during lessons, meetings, and other professional settings to minimise disruption and maintain a focused learning environment.

13.6.4. When away on:

- an off-site school trip.
- a sports fixture or match.

staff are permitted to have their mobile devices and wearable devices switched on and on their person. Staff are to only use their mobile devices for phone calls in case of emergency. The school may need to contact the member of Staff to pass on any urgent or emergency message.

13.6.5. Staff mobile phones, wearable devices and personal devices must only be used to access emails in staff areas and not in the presence of children.

13.6.6. Cameras, iPads, personal devices, mobile phones, and wearable devices with camera or recording functions are strictly prohibited in toilets or changing areas.

13.7. **Mobile Phone or Personal Device Misuse**

13.7.1. **Pupils**

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy.

13.7.2. **Staff**

- Staff must not use personal mobile phones during lessons or in the presence of pupils, unless required for operational or emergency purposes. Mobile phone use must never compromise the school's safeguarding or professional conduct policies.
- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment or School iPads will be used for this.
- The school expects staff to lead by example. Staff should ensure mobile phones are kept on silent during lessons, meetings, and other professional settings to minimise disruption and maintain a focused learning environment.
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the Child Protection and Safeguarding Children Policy, or in the staff contract of employment.

13.8. **iPads and Chromebooks (Mobile Teaching Devices)**

- Make sure that iPads / Chromebooks are locked away at the end of the day and that all are accounted for.
- Children are appointed Digital leaders.
- Head of ICT regularly conducts random searches of school iPad / Chromebook contents, checking that content is appropriate and in accordance with responsible use guidance. In addition, daily reports are provided via Securly and Impero detailing suspicious search queries.
- Guidance is provided for students and staff in our Acceptable Use Policies.

14. Cyberbullying

Ludgrove School takes Cyberbullying, as with any other form of bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the Anti-Bullying Policy and Child Protection and Safeguarding Children Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

14.1. **If an allegation of bullying does occur, the school will:**

- Take it seriously.
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider to identify the bully.
- Record and report the incident.
- Provide support and reassurance to the victim.
- Make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who

have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

15. Managing Emerging Technologies

Technology is progressing rapidly, and new technologies are emerging all the time. The school will risk-assess and conduct a Data Impact Assessment, where necessary (and in accordance with the Data Protection Policy) any new technologies before they are allowed in school and will consider any educational benefits that they might have. The school keeps up to date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

16. Artificial Intelligence (AI)

In alignment with Ludgrove School's commitment to embracing cutting-edge educational tools. Our ICT Policy outlines the strategic use of Artificial Intelligence to enrich teaching and learning processes. AI applications are employed to personalise learning experiences, providing students with tailored educational pathways that cater to their individual needs and abilities. The policy emphasizes the importance of data privacy and ethical considerations, ensuring that all AI tools used comply with relevant regulations and uphold the highest standards of security. Teachers are provided with ongoing professional development to effectively integrate AI into their pedagogical practices, enhancing both teaching efficiency and student engagement. Throughout this policy, Ludgrove School, aims to equip students with the digital literacy skills necessary for success in an increasingly AI-driven world, preparing them to be responsible and informed digital citizens. For further information, please refer to our AI Use Policy.

17. Protecting Personal Data

17.1. Ludgrove believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole school and individual progress. The school collects personal data from pupils, parents, and staff and processes it to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision. See Data Protection Policy.

17.2. For further information on how we look after your personal data, please refer to our Privacy Policy online and our Data Protection Policy.

18. Remote Access Policy

Staff can access the school network at home via Remote Desktop Protocol (RDP). All users:

- Can access a remote desktop session.
- Can access the same files and resources as they can when logged onto a school computer on-site.
- Are asked to be vigilant and to log off after use.

19. Reporting on Compliance and Effectiveness

An annual report, covering compliance with and summaries of:

- The daily reports received (at 7am) by the Head of ICT, showing the previous day's activity with children using the computers, so that any issues can be quickly investigated; examples include:
  - Any suspicious search queries using Google.
  - The length of time each child spent using the Internet.
  - Any suspicious words typed on a computer by a child.
- Using the Rewards and Conducts modules in iSAMS, produce a report of any issues involving the children and what action is taken. When an entry is made, this is copied to the child's Division Master, Houseparent, and the Head of Discipline.
- Weekly, monthly, and annual reports from Connect Systems showing the status of the Network Servers.
- The last logon time for the Parent Portal to ensure that all Parents are accessing children's Progress and End of Term Reports.

20. Breaches of Policy

20.1. Any breach of this Policy may lead to disciplinary action being taken against the staff member/s involved up to and including dismissal, in line with the School's Disciplinary Policy and Procedures. Any staff member/s suspected of committing a breach of this policy will be required to cooperate with the school's investigation, which may involve handing over relevant passwords and login details.

20.2. Staff member/s may be required to remove any social media content that the school considers to constitute a breach of this policy. Failure to comply with such a request may result in disciplinary action.

20.3. Any non-compliance will be taken seriously, logged, and investigated appropriately in line with our disciplinary policy.