ONLINE SAFETY AND RESPONSIBLE USE POLICES

Our Online Safety Policy has been written by the school, building on the Wiltshire Learning Trust Online Safety Policy template and government guidance. The content has been discussed and agreed by Senior Leadership, all staff and governors.

Ludgershall Castle Primary School identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

Online Safety Group
Lead Online Safety Officer: Mrs S Lowe (Head Teacher)
Computing Subject Lead: Mrs S McKeown
Lead Online Safety Governor: Mrs D Rowley

1.1 AUTHORISED ACCESS

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission will be sought on enrolment at Ludgershall Castle Primary School and again as each child enters Key Stage Two.

- The school receives Internet Service Provision (ISP) from School Care/ Broadband 4 and will request monitoring reports from the ISP which will be regularly checked to identify any attempts to access illegal content and should notify the local police and Wiltshire Council in these instances.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn. Each pupil and staff member will be given automatic access when starting at the school. The computing leader and head teacher will review if anybody has had their access revoked annually and keep a record of any incidents.
- Primary pupils' home-school agreement will include the Responsible Use Policy and guidance for sound, image and video for publication online. (See Appendices).
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.

- *Parents will be informed that pupils will be provided with supervised Internet access.*

1.2 FILTERING AND MONITORING

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from the youngest pupil to staff.

- A log of all staff with unfiltered access to the Internet will be kept and regularly reviewed.
- The computing lead will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents, Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider via the online safety lead (computing leader).
- Website logs will be regularly sampled and monitored by the computing lead and reported the head teacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal or may place an individual at risk must be referred to the appropriate authorities.
- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.

1.4 RISK ASSESSMENT

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2. TEACHING AND LEARNING

2.1 THE CURRICULUM

The Internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent, confident and creative users of information and communication technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed Computing is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Whilst Internet access is an entitlement, users will need to show a responsible and mature approach to its use or this privilege may be removed.
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- An online safety curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst pupils.
- Education about safe and responsible use will precede internet access.
- Pupils input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Pupils will be supported in reading and understanding the Responsible Use Policy in a way which suits their age and ability.
- All users will be informed that network and Internet use will be monitored.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within all subject areas.
- External support will be used to complement and support the school's internal online safety education approaches.
- The school will implement peer education to develop online safety as appropriate to the needs of the pupils through the use of Digital Leaders.

2.2 ENHANCING TEACHING AND LEARNING

Benefits of using the Internet in education include:

- *Access to a variety of worldwide educational resources;*
- *Inclusion in the National Education Network which connects all UK schools;*
- *Educational and cultural exchanges between pupils worldwide;*
- *Vocational, social and leisure use in libraries, clubs and at home;*
- *Access to experts in many fields for pupils and staff;*
- *Professional development for staff through access to national developments;*

- *Educational materials and effective curriculum practice;*
- *Collaboration across networks of schools, support services and professional associations;*
- *Improved access to technical support including remote management of networks and automatic system updates;*
- *Access to learning wherever and whenever convenient.*

2.3 EVALUATING CONTENT

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable site or content they consider to be inappropriate, the URL (address) and content should be reported to their ISP.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.

2.4 THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS IN SCHOOL

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address the risks.
We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.
The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

- The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in the staff acceptable use agreement, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- AI tools may be used to assist teachers in the assessment of learners' work, identification of areas for improvement and the provision of feedback. Teachers may also support learners to gain feedback on their own work using AI
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.

Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Behaviour Policy.

3. COMMUNICATION AND CONTENT

3.1 WEBSITE CONTENT

Publication of any information online should always be considered from a personal and school security viewpoint.

- The point of contact on the school website should be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from individuals, parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully and will not enable individuals to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified, either individually or through aggregated pieces of information.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 LEARNING PLATFORMS

An effective learning platform (LP) or virtual learning environment (VLE) can offer schools a wide range of benefits to teachers, pupils and parents, as well as support for management and administration.

- All users will be required to use an age appropriate password to access the relevant content of the LP which must not be shared with others.
- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of individual and intellectual property and will upload only appropriate content to the LP.
- When a user leaves the school their account or rights to relevant content areas will be disabled or transferred to their new establishment.

3.3 MANAGING E-MAIL

E-mail is an essential means of communication for staff. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

Children at Ludgershall Castle Primary School learn about the safe practice of email using age appropriate resources to communicate with each other and in simulated situations such as on a LP.

Children are not provided with email accounts to limit the risk of inappropriate content being sent to them.

Staff accessing school email accounts will need to ensure they take care to do so responsibly referring to the RUP.

- Sending images without consent, explicit images, messages that cause distress and harassment to others or are considered significant breaches of school RUP and will be dealt with accordingly.
- Pupils must immediately tell a responsible adult if they receive offensive or distressing e-mail.
- Staff and governors must use secure e-mail for all professional communications and wherever possible, this should be via an official school provided email account
- E-mail sent to an external organisation should be written carefully and where appropriate, authorised before sending, in the same way as a letter written on school headed paper.

3.4 ON-LINE COMMUNICATIONS AND SOCIAL MEDIA.

On-line communications, social networking and social media services may be filtered in school by their ISP but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Schools have a key role to teach young people about the importance of how to communicate safely and respectfully online, keeping personal information private.

- Users will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Users must not reveal personal details of themselves or others in online communication, including the tagging of photos or video, or to arrange to meet anyone.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and only operate with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the school community should publish specific and detailed private thoughts about the school, especially those that may be considered threatening, hurtful or defamatory.

- Parents wishing to photograph or video at an event they should be made aware of the schools expectations and be required to comply with the schools RUP as a condition of permission to photograph or record. 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 students / pupils in the digital / video images.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Responsible Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.
- Ludgershall Castle Primary School's official social media channels are:

  Facebook page: https://www.facebook.com/LudCastlePri/

  Twitter: https://twitter.com/ludcastlepri
- Official use of social media sites by the school/setting will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be risk assessed and formally approved by the head teacher and computing lead.
- Official school/setting social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- Staff will use school/setting provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 1998, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying and child protection.
- Images or videos of children will only be shared on official social media sites/channels in accordance with the image use policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.

- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Public communications on behalf of the school/setting will, where possible, be read and agreed by at least one other colleague.
- Official social media channels will link back to the school/setting website and/or Acceptable Use Policy to demonstrate that the account is official.
- The school/setting will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

3.5 MOBILE DEVICES (INCLUDING BRING YOU OWN DEVICE-BYOD)

Mobile devices refer to any device that provides access to the internet or internal network for example, tablet (Apple Android, Windows, and other operating systems) e-readers, mobile phone, iPad, iPod touch, digital cameras.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet accesses all common features. A policy which prohibits users from taking mobile devices to school could be considered to be unreasonable and unrealistic for schools to achieve. Due to the widespread use of mobile devices it is essential that schools take steps to ensure that these devices, both personally and school owned, are used responsibly.

Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- users have access to resources to support learning and teaching
- users should be given clear boundaries on responsible and professional use

- Mobile devices that are brought in to school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- School staff authorised by the Head teacher may search pupils or their possessions, and confiscate any mobile device they believe is being used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on the mobile device relates to a criminal offence, the device will be handed over to the Police for investigation.
- Sending abusive or inappropriate messages or content is forbidden by any user within the school community.
- Mobile devices may be used during lessons or formal school time as part of approved and directed curriculum based activity.
- Mobile devices are not permitted to be used in certain areas or situations within the school site e.g. changing rooms or toilets, swimming pools, situations of emotional distress etc.
- Where staff may need to contact children, young people and their families within or outside of the setting in a professional capacity, they should only do so via an approved school account (e.g. e-mail, phone, social media) In exceptional circumstances there may be a need to use their own personal devices and account; this should be notified to a senior member of staff ASAP
- Staff will be provided with school equipment for the taking photos or videos of pupils linked to an educational intention. In exceptional circumstances staff may need to use personal devices

for such a purpose and when doing so, should ensure they comply with the schools Responsible Use Policy.

- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school wireless provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- The school will take steps to monitor responsible use in accordance with the Responsible Use Policy
- Staff will not use personal devices such as mobile phones, tablets, smart watches or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
- Staff personal mobile phones and devices will be kept in personal lockers in a staff room.
- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school/settings acceptable use policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- The school will ensure appropriate information is provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.
- Signed copies of RUP will be kept in the main office. Visitors will complete signing in book to acknowledge the correct use of personal devices or be asked to read the visitor RUP if accessing school systems or equipment.

3.6 VIDEO CONFERENCING

Video conferencing (including FaceTime, Skype and Lync) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible should take place using the school's wireless system.

- Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupils' age and ability.

3.7 EMERGING TECHNOLOGIES

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment should be completed on each new technology and assessed for effective and safe practice in classroom use. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.8 CYBER BULLYING

Cyber bullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff, parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyber bullying (along with all other forms of bullying) of or by any member of the school community will not be tolerated. Full details are set out in the school's behaviour, anti-bullying and child protection policies, which should include:

- Clear procedures in set out to investigate incidents or allegations of cyber bullying.
- Clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the ISP and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school's Online Safety ethos.

3.9 DATA PROTECTION

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

The school's Data Controller is Mrs J Beaumont. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils / students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
- When personal data is stored on any portable computer system, USB stick or any other removable media:

· the data must be encrypted and password protected,
· the device must be password protected,
· the device must offer approved virus and malware checking software, and
· the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

- The school has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

3.10 CYBER SECURITY

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage"

- the school has reviewed the DfE Cyber security standards for schools and colleges and is working toward meeting these standards
- the school will conduct a cyber risk assessment annually and review each term
- the school, (*in partnership with their technology support partner),* has identified the most critical parts of the school's digital and technology services and sought assurance about their cyber security
- the school has an effective backup and restoration plan in place in the event of cyber attacks
- the school's governance and IT policies reflect the importance of good cyber security
- staff and Governors receive training on the common cyber security threats and incidents that schools experience
- the school's education programmes include cyber awareness for learners

- the school has a business continuity and incident management plan in place
- there are processes in place for the reporting of cyber incidents. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

3.11 USE OF PASSWORDS

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- All pupils are provided with their own unique username and private passwords to access school systems. Pupils are responsible for keeping their password private.
- We require staff and pupils to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords every academic year.

4 IMPLEMENTATION

4.1 Policy in Practice-Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's online safety teaching and awareness-raising it is important to discuss the key features with pupils / students as appropriate for their age. Pupils may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network and Internet use will be monitored.
- Online Safety teaching should be integral to the curriculum and raise the awareness and importance of safe and responsible internet use amongst pupils.
- Online Safety teaching will be included in the PSHE, Digital Citizenship and/or Computing and cover safe use at school and home.
- Online Safety rules and/or copies of the Responsible Use Policy will be on display in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

4.2 POLICY IN PRACTICE- STAFF

It is important that all staff feel confident to use new technologies in teaching and the School Online Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies.

Particular consideration must be given when members of staff are provided with devices by the school which may be accessed outside of the school network. Schools must be clear about the safe and appropriate uses of their school provided equipment and have rules in place about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of school information. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their senior leader to avoid any possible misunderstanding.

- The Online Safety Policy will be provided to and discussed with all members of staff and Responsible User Policy signed for compliance.
- Staff should be aware that Internet traffic is monitored (and automatically reported by the ISP) and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.3 POLICY IN PRACTICE- PARENTS

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

Schools may wish to refer parents to websites referred to in the references section of this document.

- Parents' attention will be drawn to the Online Safety Policy and Responsible User Policy (RUP) in newsletters, school prospectus and Website.
- A partnership approach with parents will be encouraged. This could include offering parent evenings, demonstrations, practical sessions and suggestions for resources and safer Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

4.4 HANDLING OF COMPLAINTS

Parents and teachers must know how and where to report incidents in line with the school complaints policy and complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the Internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept, e.g. e-mails saved or printed, text messages saved etc.

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Policy created: 29th November 2016
Date of review: November 2025
Date of next review: November 2026

Ludgershall Castle Primary School

Responsible Use Policy

Dear Parents,

As part of your child's curriculum and the development of Computing, Ludgershall Castle Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Use and sign and return the consent form so that your child may use the Internet and ICT equipment at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, School Care Broadband operates a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Mrs S Lowe

Headteacher

Ludgershall Castle Primary School

Responsible Use Policy

These rules help us to stay safe when using technology and accessing the Internet.

- I will take care when handling the school ICT equipment and only use the computers and tablets when a teacher has given me permission.
- I will ask for help if I get lost or confused when using the ICT equipment.
- I will always ask permission from my teacher and the person/people involved before taking photos or videos.
- I will only access the apps or websites that my teacher has asked me to and will check before using any others.
- I will ask permission before using the Internet.
- I will keep my passwords and log in details secret and not share them.
- I will only open or delete my own files.
- I understand that I must not bring into school and use software or files without permission.
- I will only e-mail and open attachments from people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I understand that I must never give out any of my personal details or arrange to meet with anyone that I talk to on the internet.
- If I see anything I am unhappy with or I receive messages I do not like, and tell an adult immediately.
- I understand that the school may check my computer files, e-mails I send and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet, computers or tablets.
- The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. School Care/ Broadband 4 monitors all Internet use and will notify the police and Local Authority if an illegal website is accessed.

Ludgershall Castle Primary School

Responsible Use Policy

Please complete, sign and return to the school office

Parent's Consent for Internet Access

I have read and understood the school rules for responsible Internet use and ***give permission for my son / daughter to access the Internet***. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***
Please print name:	

Queries regarding this form should be addressed to the Headteacher at Ludgershall Castle Primary School.

Responsible Use Policy for Ludgershall Castle Primary School Staff/ Governors and Visitors.

(This should be agreed with reference to the Online Safety Policy)

Staff Laptop use:

1. The laptop remains the property of Ludgershall Castle Primary School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Ludgershall Castle Primary School staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Ludgershall Castle Primary School. Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the headteacher). The laptop must be returned, restored to its original condition with any personal files removed.
4. When in school and not being used, the laptop must be logged off by the user.
5. Whenever possible, the laptop must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used then it must be checked to ensure it is free from any viruses.
10. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
11. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
12. Students must never use the laptop.
13. If any fault occurs with the laptop, it should be referred immediately to the Network Manager.
14. The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

I agree with the terms of 'Staff Laptop Use' (Initials) …… This does not apply to me [ ]

Responsible use of e-mail, network and Internet use:

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
   - Access offensive website or download offensive material.
   - Make excessive personal use of the Internet or e-mail.
   - Copy information from the Internet that is copyright or without the owner's permission.
   - Place inappropriate material onto the Internet.
   - Will not send e-mails that are offensive or otherwise inappropriate.
   - Disregard my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the laptop and school network.
   - Access the files of others or attempt to alter the computer settings.
   - Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
   - Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Ludgershall Castle Primary School.

2. I will only access the system with my own name and registered password, which I will keep secret.
3. I will inform the Headteacher as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the Internet sites I visit.
6. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher.
7. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
8. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Network Manager.
9. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
10. I will report immediately to the headteacher any unpleasant material or messages sent to me.
11. I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
12. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
13. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
14. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
15. I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.
16. All staff to have an encrypted memory stick to save, transfer and store school data.

I agree with the terms of 'Responsible use of e-mail, network and Internet' (Initials) …… This does not apply to me [ ]

Use of One Drive:

1. I will only use One Drive accounts to save and store files and media that are associated with school and my work.
2. I will not share the password for the accounts with anyone other than staff of the school.
3. When using One Drive out of school this should be done on a device that has been issued by school.
4. If a personal device is used to access One Drive accounts the passwords should not be saved and it should be logged in and out of for each use.

I agree with the terms of 'Use of One Drive' (Initials) …… This does not apply to me [ ]

Use of mobile devices:

1. Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school.
2. Members of staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a

professional capacity. Any pre-existing relationships which could compromise this will be discussed with leaders/managers.

3. Staff will not use personal devices such as mobile phones, tablets, smart watches or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
4. Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.
5. Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policy and RUP.
6. Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
7. Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
8. Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
9. Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
10. If a member of staff breaches the school/setting policy then disciplinary action will be taken.
11. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
12. Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school/settings allegations management policy.

I agree with the terms of 'Use of mobile devices' (Initials) …… This does not apply to me [ ]

Use of iPads:

1. All iPads remain the property of Ludgershall Castle Primary School and is for use only by staff and children of Ludgershall Castle Primary. They must not be loaned to other adults.

2. All iPads that are assigned to staff are to be password protected and only to be used by the person assigned to that iPad especially when it is off site.

3. The children's iPads are electronically linked to school systems. They can be used without a password and may be storing picture and video images of pupils along with other personal information. This means you must fully comply with high standards of data protection outlined in the Online Safety Policy when using them.

4. You (and only you) may take an iPad assigned to you off-site if you plan to use it in a way that will benefit the school. If you don't have an assigned iPad you should agree with the computing lead/ head teacher before taking an iPad off site. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home but

excludes theft from your car or from other establishments. Should you leave the iPad unattended and it is stolen you will be responsible for its replacement and may need to claim this from your own insurance company.

5. Loss or damage of a device should be reported to the school's Computing Lead immediately. If necessary the device will be remotely locked or wiped.

6. iPads are expensive and fragile items and their use must be supervised at all times. The school's iPads should only be used when the teacher believes that all pupils present are capable of using them sensibly.

7. You are responsible for looking after iPads that you use. When left unattended they must be locked in a secure cupboard in your classroom or returned to the iPad station.

8. These iPads are configured with certain restrictions in place. You must not try to make changes to the device settings that are passcode protected.

9. You may not download apps to the iPads. If you believe there is an app that would benefit your teaching and the children's learning then please speak to the Computing Lead.

10. Use of the iPad must adhere to data protection, computer misuse and health and safety rules. Failure to do so may lead to disciplinary action.

11. When using iPads with children the activity must be structured and clear expectations and rules should be shared with the class to avoid coming into contact with inappropriate age related content.

12. After each use teachers/pupils should close all apps that they have been using to ensure that it is ready for the next group.

13. iPads will be kept together in the docking stations and an adult will arrange to collect and return the iPads for use.

14. When returning iPads an adult will check if the iPad needs charging and will report any damages/ concerns to the computing lead.

15. The computing lead will ensure that all software is up to date and will install/remove any apps that are needed.

16. This agreement covers the current academic year only. A new agreement must be signed at the start of each academic year.

I agree with the terms of 'Use of iPads' (Initials) …… This does not apply to me [ ]

I have read this agreement and fully understand that I need to adhere to all elements that I have signed.

Staff Member Name: .....

Signature: ..... Date: .....

NB: The Computing Lead is Mrs S McKeown