Acceptable Use Agreement: Monk Fryston Primary School

- **Foundation / Key Stage 1**
- **Pupil Acceptable Use Agreement / eSafety Rules**
  - I will only use ICT in class when an adult tells me
  - I will only click on icons and use programs that I know are for me
  - I will only go on the internet with an adult near
  - I will not tell other people my ICT passwords
  - I will only open/delete my own files
  - I will tell an adult if something happens that I don't understand or like
  - I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
  - I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher straight away
  - I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
  - I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety

Monk Fryston Church of England Primary School
Chestnut Green
Monk Fryston
Leeds
LS25 5PN
Telephone: 01977 682388
Fax: 01977 680564
Email: admin@mf.starmat.uk
Headteacher: Mr R M Weights B.Ed, FHA

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Weights.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

We have discussed this document with our child and agree to follow the eSafety rules and to support the safe use of ICT at Monk Fryston Primary School.

Foundation /KS1 Pupil name ………………………………….. Year Group………………….

Parent/ Carer Signature ………………………..………………………….

Date ……………………………….

PLEASE SEE ACCEPTABLE USE AGREEMENT OVERLEAF

- **Key Stage 2 Pupil Acceptable Use Agreement / eSafety Rules**
    - I will only use ICT in school for school purposes
    - I will only use a school provided e-mail address when e-mailing from school
    - I will only open e-mail attachments from people I know, or who my teacher has approved
    - I will not tell other people my ICT passwords
    - I will only open/delete my own files
    - I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
    - I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
    - I will not click suspicious links or open files that I do not trust.
    - I will not create or share fake images, videos, or recordings of others.
    - I will report cyberbullying, scams, fake accounts or suspicious messages immediately.
    - I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
    - I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
    - I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
    - I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
    - I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
    - I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
    - I will not sign up to online services until I am old enough
    - I understand that Artificial Intelligence (AI) tools must only be used if my teacher says I can and I must not pretend AI work is my own.

Monk Fryston Church of England Primary School
Chestnut Green
Monk Fryston
Leeds
LS25 5PN
Telephone: 01977 682388
Fax: 01977 680564
Email: admin@mf.starmat.uk
Headteacher: Mr R M Weights B.Ed, FHA

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr Weights.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

We have discussed this document with our child and agree to follow the eSafety rules and to support the safe use of ICT at Monk Fryston Primary School.

KS2 Pupil name …………………………………………………………. Year Group………….

KS2 Pupil Signature ……..………………………..

Parent/ Carer Signature ……..……………………..……………………………

Date ………………………………

PLEASE SEE ACCEPTABLE USE AGREEMENT OVERLEAF

Acceptable Use Agreement: Monk Fryston Primary School

Acceptable Use Statement

The computer system is owned by the school. “The computer system” means all computers and associated equipment belonging to the school, whether part of the school’s integrated network, stand-alone, or taken offsite. Furthermore, it includes the ‘cloud space’ which is under contract through the school – Google Drive and Office 365 Cloud Storage systems.

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences; or allow adults to enhance their own professional development. The school recognises that technologies such as the Internet and e-mail will have a profound effect on children’s education and staff professional development in the coming years and the school’s Internet Access Policy has been drawn up accordingly.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is expressly forbidden.

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any Internet sites visited.

All members of staff, students on placement, supply teachers etc must read a copy of this policy statement before a system login password is granted. All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use.

Internet Access Policy Statement

All Internet activity should be appropriate to staff professional activities or the children’s education;

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The Internet is available for access by staff and children throughout their hours in school;
- Activity that threatens the integrity of the school’s computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content. The same professional levels of language should be applied as for letters and other media. Only school email addresses should be used for school official business;
- Use of the school’s Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school’s network is the property of the school and making unauthorised copies of materials contained thereon maybe in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights;
- Use of materials stored on the school’s network for personal financial gain is excluded;
- Posting anonymous messages and forwarding chain letters is excluded;
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden;
- All web activity is monitored, including the language or image content of e-mail, therefore it is the responsibility of the user to ensure that they have logged off the system when they have completed their task;

- Children must not be given unsupervised access to the Internet. For the purposes of this policy, “supervised” means that the user is within direct sight of a responsible adult;

- The teaching of Internet safety is included in the school’s ICT Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the school’s computer systems;

- All children must understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.

Internet and System Monitoring

Through the *Smoothwall filtering and monitoring service,* all Internet activity is monitored by the system. It is the responsibility of the ICT co-ordinator to review this activity periodically. It is the duty of the ICT co-ordinator to report any transgressions of the school’s Internet policy and/or use of obscene, racist or threatening language detected by the system to the Headteacher. Occasionally, it may be necessary for the ICT co-ordinator to investigate attempted access to blocked sites, and in order to do this, the ICT co-ordinator will need to set his/her Internet access rights to “Unrestricted”. Whenever this happens, this should be recorded with the Headteacher.

All serious transgressions of the school’s Internet Access Policy are recorded with the Headteacher.

Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including removal of Internet access rights; computer system access rights; meetings with parents or even exclusion; in accordance with the severity of the offence and the school’s Behaviour Policy.

Breaches of Internet Access Policy by staff will be reported to the Headteacher and will be dealt with according to the school’s and LA’s disciplinary policy, or through prosecution by law.

Monitoring systems may also use automated safeguarding and AI-based detection tools to identify risk indicators.

Internet Publishing Statement

The school wishes the school’s website, to reflect the diversity of activities, individuals and education that can be found at our school. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child’s own verbal consent; (See pro forma)

- Surnames of children should not be published, especially in conjunction with photographic or video material;

- No link should be made between an individual and any home address (including simply street names);

- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

- No AI-generated or digitally manipulated media of pupils or staff may be published without explicit leadership approval.

Use of Portable Equipment

The school provides portable ICT equipment such as laptop computers, colour printers and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities. This policy applies equally to wearable technology, smart devices, tracking devices and emerging technologies capable of recording, communicating or transmitting data.

Exactly the same principles of acceptable use apply as in the Acceptable Use Statement above.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the ICT co-ordinator;

- Certain equipment will remain in the care of the ICT co-ordinator, and may be booked out for use according to staff requirements. Once equipment has been used, it should be returned to the resource area;

- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use Statement and Internet Access Policy and the equipment is fully insured from the moment it leaves the school premises. Note: our school insurance policy provides cover for equipment taken offsite, provided it is looked after with due care, i.e. not left in view on a car seat etc;

- Employees should not use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher; they should only used for professional purposes.

- Staff must not store school data on personal cloud storage platforms or personal devices unless authorised and encrypted.

- Any costs generated by the user at home, such as phone bills, printer cartridge etc. are the responsibility of the user;

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc.) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it;

- If an individual leaves the employment of the school, any equipment must be returned;

- Staff may install software on laptops to connect to the Internet from home. If in doubt seek advice;

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software;

- All staff are encouraged to make use of the school's anti-virus software for installation on any computers at home that they routinely use for school work.

- Transfer of pupil data must be by use of encrypted usb drives or encrypted e-mail attachment. These are available for order via the ICT Coordinator. Employees are not permitted to use personal portable media for storage of sensitive school related data/images (e.g. USB stick) without the express permission of the Headteacher.

- Staff use of personal mobile devices to collect or send e-mail/text messages or browse the internet during school hours is strictly limited to non-contact time; the same rules for acceptable use/content apply to these personal devices when on school site in case the device is misplaced and handled by pupils. Staff should not use personal telephones to text or for telephone conversations during contact time or when in meetings. Ringtones should be set to silent or phones out of earshot during contact time or when in meetings. Personal devices may, in exceptional circumstances, be used to capture pupil images but these must be removed and stored on school systems at the earliest possible opportunity.

Social Networking and Other Means of Communication

- Staff should ensure that their use of web 2 technologies, including social networking sites, such as Facebook, does not question or bring their professional role into disrepute.
    - Staff are advised to consider, and set appropriately, their privacy settings on such sites.
    - Staff should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
- Staff should not communicate with pupils, in relation to either school or non school business, via web 2 technologies. Members of staff should only communicate with pupils using the appropriate LA/school learning platforms or other systems approved by the Headteacher.

- Communication with pupils (for work feedback) must only take place via school-approved platforms (Google Classroom). Messaging apps, private chat services or personal social media must not be used.

- Staff are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or un-blocked personal telephone numbers, without specific permission from the Headteacher.
- Staff should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Staff must ensure that all electronic communication with pupils and staff is compatible with their professional role.

Artificial Intelligence, Emerging Technology & Digital Safety

The school recognises that artificial intelligence and emerging technologies are increasingly integrated into educational tools and online platforms.

Use of AI must be safe, ethical, transparent and age-appropriate. It must comply with the YLT AI policy.

Staff Responsibilities

- Staff must not input personal, confidential or pupil data into public AI systems.
- Staff must supervise pupil use of AI tools.
- Staff must verify accuracy of AI-generated information before use in teaching.
- Staff must ensure pupils understand when AI is used in their learning.

Pupil Responsibilities

- AI must not be used to cheat, plagiarise or misrepresent work.
- AI must not be used to generate harmful, offensive or misleading content.

Remote Learning & Online Lesson Conduct (New Section 2025)

These expectations apply whenever pupils access school systems outside the school site.

- Online lessons must not be recorded or shared. - Meeting links must not be shared. - Pupils must behave online as they would in class. - Appropriate clothing and surroundings must be maintained during video sessions. - Parents should support safe supervision of online learning at home.

Data Protection & Cloud Use

School data must only be stored on approved platforms. Personal email or cloud accounts must not be used for school business.

Any suspected data breach must be reported immediately to the Headteacher or Data Protection Lead.

Data must be retained, shared and deleted in accordance with data protection law and school retention schedules.

Online Behaviour & Safeguarding

The school recognises that online behaviour outside school may still impact safeguarding and wellbeing within school.

Sanctions may apply for online behaviour outside school where it affects pupils, staff or the school community.

Prohibited behaviours include:

- Cyberbullying
- Harassment or intimidation
- Sharing harmful content
- Creating fake accounts
- Manipulating images, audio or video of others.

Approval of Digital Platforms

All digital platforms, apps or online tools used for teaching must be approved by school leadership prior to use.

New systems must be assessed for:

- Safeguarding compliance
- Data protection compliance
- Age appropriateness
- Security standards

Policy Review Statement

This policy will be reviewed every three years or sooner in response to technological, legal or safeguarding developments.