Heather Primary School – E-SAFETY POLICY

This policy was approved by the Governing Body of Heather Primary	**Date – 19-09-24**
Signed	**Chair: Dawn Guzzetta**

Version	Date	Author	Reason For Change
0.2	February 21	MM/GK	Updated IT support and broadband provider
0.3	February 23	MM	Annual review, update of signatory and DSLs
0.4	Sept 24	MM/GK	Clarity over monitoring

Review Frequency	Next Review Date
Annual	September 2025

The implementation of this E-Safety policy will be monitored by the: Headteacher
Serious E-Safety concerns and incidents must be reported to; Maxine Michalowski (DSL), Pippa Barton, Linda Thornley (Deputy DSLs)

Heather Primary School E-Safety Policy

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to E-Safety. E-Safety relates to accessing the Internet and the use of other digital technologies. It highlights the need to educate pupils about the benefits and risks of using technology and the Internet and provides safeguards and awareness for users to enable them to control their online experience.

The school's E-Safety policy operates in conjunction with other policies including Safeguarding, Behaviour, Data Protection, Child Protection and Anti-Bullying. Also, Acceptable Use Polices, Social Media Policy and Laptop Policy are listed as appendices in this document.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of E-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from RM Education who provide the internet connectivity, managed firewall and web filtering services for the school network.

Scope of Policy

This policy applies to:

- All teaching and support staff (including peripatetic staff)
- School governors and volunteers
- Children within the school
- Visitors and community organisations and users.

Teaching and Learning

Why Internet and use of new technologies is important

- The Internet is an essential resource in 21st century 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils use the Internet widely inside and outside of school and need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online.

Internet use will enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Allows for access to worldwide educational resources and contacts.

Pupils will be taught how to evaluate Internet content

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to DSL and GSKS, our IT Support provider.

How will Internet access be authorised?

- The school allocates Internet access for staff and pupils on the basis of educational need.
- Authorisation is as individuals and usage is fully supervised.
- Normally all pupils will be granted Internet access.
- Parental permission is required for Internet access in all cases as new pupils join the school.
- All staff must read and sign the Code of Conduct/Acceptable Use Policy before using any school ICT resource.
- Parents will be asked to sign and return a consent form for pupil access.

Users (staff, pupils, visitors, volunteers, governors etc) are not allowed to:

Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children
- Promoting discrimination of any kind
- Promoting racial or religious hatred
- Promoting illegal acts
- Any other information which may be offensive, embarrassing or upsetting to peers or colleagues (i.e cyberbullying) e.g. abusive text or images; promotion of violence; gambling; criminally racist or religious hatred material

The School recognises that in certain planned curricular activities, access to otherwise deemed inappropriate sites may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned and recorded and permission given by senior leaders, so that the action can be justified, if queries are raised later. Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the Police:

- Images of child abuse (images of children whether they are digital or cartoons, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Other criminal activity

In addition, users are not allowed to:

- Use school broadband or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves schools broadband or members of Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of schools broadband or member Local Authorities or adversely impact on the image of school's broadband.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of school's broadband, or to school's broadband itself;
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships;
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and

receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet;

- Use the Internet for soliciting, revealing confidential information or in any other way that could reasonably be considered inappropriate.
- Transmit unsolicited commercial or advertising material either to other user organisations, or to organisations connected to other networks, save where the material is embedded within, or is otherwise part of, a service to which the member of the user organisation has chosen to subscribe.
- Assist with unauthorised access to facilities or services accessible via school's broadband.
- Undertake activities with any of the following characteristics:
- Wasting staff effort or networked resources, including time on end systems accessible via the school's broadband network and the effort of staff involved in support of those systems;
    - corrupting or destroying other users' data;
    - violating the privacy of other users;
    - disrupting the work of other users;
    - using the school's broadband network in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
    - continuing to use an item of networking software or hardware after school's broadband has requested that use cease because it is causing disruption to the correct functioning of school's broadband.
    - other misuse of the school's broadband network, such as introduction of viruses.

- Use any new technologies in any way to intimidate, threaten or cause harm to others. Moreover, mobile technologies should not be used to access inappropriate materials or encourage activities that are dangerous or illegal.

How is E-Safety taught in the curriculum?

E–Safety is taught as an ICT lesson activity (see Somerset IT Scheme), through our PSHE scheme of work and our Protective Behaviours Units.

All users are informed that network and Internet use will be monitored.
Pupil instruction in responsible and safe use should precede Internet access every time they go online.
Safe and responsible use of the internet and technology will be reinforced across the curriculum.
Particular attention will be given where pupils are considered to be vulnerable.

How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher. If the complaint is about the Headteacher, this should be reported to the Chair of Governors.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaint's procedure. Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the LADO, Police and Leicestershire and Rutland Safeguarding Children Board to establish procedures for handling potentially illegal issues.
- Any issues where inappropriate or illegal use of technologies by Adults (Staff and Volunteers) will be dealt with according to the school's Disciplinary and Child Protection procedures. Serious breaches may lead to the incident being reported to the Police or other regulatory bodies for examples, illegal internet use or child protection concerns.
- Any issues where inappropriate or illegal use of technologies by a child/young person – the child/young person will be disciplined according to the school behaviour policy. Serious breaches may lead to the incident reported to the Police or other regulatory bodies for examples, illegal internet use or child protection concerns.

How is the Internet used across the community?

- We recognise that children can access the internet outside of school and offer support and advice to parents on internet safety though regular information sent home with children and through advice in our newsletters.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- The school will hold E-Safety assemblies for all children.
- Heather Primary School E-Safety Policy and E-Safety information will be shared with parents regularly throughout the year at parent meetings and workshops and through newsletters and school website links.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School E–Safety Policy in newsletters etc.
- A partnership approach with parents will be encouraged. This will include parent meetings with demonstrations and suggestions for safe home Internet use.
- Parents will be requested to sign an Acceptable Use Policy as part of the school's on entry procedures.
- We also appreciate that there may be some parents who are concerned about the use of the new technologies in school. In such circumstances school staff will meet with parents and carers to discuss their concerns and agree upon a strategy that will allow their child to fully access the curriculum, whilst remaining safe.

How will Cyberbullying be managed?

Cyberbullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DfE 2007.
It is essential that pupils, staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond. The school will make use of expert advice on such issues. The DfE and Childnet have produced resources and guidance that will be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying
Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
There are clear procedures in place to investigate incidents or allegations of cyberbullying:

- Pupils, staff and parents/carers will be advised to keep a record of the cyberbullying as evidence.
- The school will take steps to identify cyberbullying behaviour, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include: asking the perpetrator to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers will be informed, and the Police will be contacted if a criminal offence is suspected.

Sexting and Pornography

Sexting – Children in Year 5 and 6 will be informed about the implications of sexting and how, once a picture has been sent, this image can never fully be removed from the World Wide Web.
Pornography – many children will come across some type of pornographic content when searching the Internet. Children will be taught about what to do if they access this type of material and who to speak to.

The Prevent Duty and E-Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe online. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well-being of any pupil is being compromised.

Reporting Abuse

There will be occasions when either a pupil or an adult within the school receives an abusive email or accidentally accesses a website that contains abusive material. When such a situation occurs, the expectation of the school is that the pupil or adult should report the incident immediately.

The School also recognises that there will be occasions where pupils will be the victims of inappropriate behaviour that could lead to possible or actual significant harm. In such circumstances the school will take the reporting of such incidents seriously and where judged necessary, the Designated Safeguarding Lead for Child Protection within the School will seek advice from the LADO (Local Authority Designated Officer) and refer details of an incident to Children's Social Care or the Police.

- The School, as part of its safeguarding duty and responsibilities will, in accordance with Leicestershire and Rutland Safeguarding Children Board to assist with and provide information/advice in support of child protection enquiries and criminal investigations.

Published content and the school website, Twitter account and WEDUC

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission (GDPR permission form) for parents/carers will be obtained before photographs of pupils are published on the school website. Children's full names will not be used.

Monitoring and Filtering

The school will work with GSKS to ensure that age-appropriate filters and systems are in place to protect pupils and that these are reviewed, and improvements implemented.

- If staff or pupils discover unsuitable sites, the URL must be reported to DSL and GSKS
- Any material that members of staff believe is illegal must be reported to the Headteacher who will inform the appropriate agencies.
- The school keep up to date with new technologies, including those relating to mobile phones and handheld devices, and develop appropriate strategies.

Emerging technologies will be examined for educational benefit and the Head teacher in consultation with staff will give permission for appropriate use.

Our IT technician monitors and reports on an ongoing basis of any issues arising from filtering and monitoring incidents. Last year the only issues were minor behaviour issues related to being on-task which is outside the scope of the policy and was acted upon by the supervising adult. These low-level behaviour incidents showing up in our filtering and monitoring data shows that the systems in place are functional giving us confidence that issues that would come within scope would be identified. I periodically prompt to confirm that no issues have arisen if I haven't received any reports.

Appendices

1. Acceptable Use Policy – staff/volunteers and children
2. Mobile Phone Use
3. Social Media Policy
4. Laptop Policy
5. Devise Loan Agreement

Appendix 1

Heather Primary School Acceptable Use Policy for Primary Pupils

To keep me safe whenever I use the internet or email, I promise…

- to keep my username and password private and not to use anyone else's
- to keep all personal information private

- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting

- to tell someone I trust if someone asks to meet me offline

When using computer equipment in school…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules…

- I understand that the school's behaviour guidelines will be followed

I have read and understand this policy and agree to follow it.

Name of pupil _____

Signed _____ Date _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the internet.

Parent/Carer signature _____ Date _____

Heather Primary Acceptable Use Policy for Staff and Volunteers

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

- I understand that the Heather Primary School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / WEDUC) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies (see social media policy).
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using Heather Primary School equipment. I will also follow any additional rules set by the Heather Primary School about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I may use personal email addresses on the school ICT systems to access school related items.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- Staff and Governors will only use their professional Microsoft 365 email account for school business.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- Any flashdrives, external hard drives must be encrypted by GSK/School Office before use in school.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)

I understand that I am responsible for my actions in and out of Heather Primary School.

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action, this could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: _____

Signed: _____

Date:_____

Appendix 3

Heather Primary Social Media Policy (using guidance from Social Media Policy template LTS)

This guidance applies to all staff, including Head Teachers / Principals, Teachers and all Support Staff regardless of whether they are permanent, fixed term, casual or agency or volunteers. It provides guidance on what measures are to be taken to ensure the safe use of social media and defines what is considered to be inappropriate conduct when using social media/internet sites for both professional and personal purposes.

Breaches of this guidance may be dealt with via the school's disciplinary policy or where it is appropriate will be referred to the police.

For the purposes of this guidance Headteacher will be referred to as Headteacher and Heather Primary School will be referred to as school.

Documents to support this Guidance:

In addition, this Guidance should also be read in conjunction with the school's code of conduct, /e-safety policy, school's disciplinary procedures. The school will also take into account any current and relevant legislation.

Purpose

The primary purpose of this guidance is to clarify how all employees should conduct themselves when using all forms of social media whether this is done through the school's media or personal media, in work time or in an individual's own time. The aim being to minimise the risk employees may place themselves and pupils in when they choose to write about their work or matters relating to the school and/or their personal lives.

This in turn will minimise situations where safeguarding concerns could arise, employees' integrity or professional standing could be undermined, professional relationships with colleagues and pupils are compromised or the school and the Local Authority brought into disrepute.

Additionally, adhering to the Guidance reduces the risk of employees inadvertently contravening sections of the Data Protection Act or falling foul of any breaches of confidentiality, privacy, libel, defamation, harassment and copyright laws.

Whilst this Guidance is not intended to prevent employees from using social media sites, it does aim to make employees aware of the risks they could face whilst doing so and highlight what is deemed to be unacceptable when sharing information about their professional and/or personal life. Employees should be encouraged to report any concerns that they have regarding content placed by employees on social media sites to the Head teacher.

When an employee(s) wishes to create a work-related social media site they must discuss this with and obtain the relevant approval from the Head teacher. Creators of these groups are responsible for monitoring the content of the site and ensuring that it is appropriate and not in breach of any of the terms in this Guidance.

Application of the Guidance

The Social Media Guidance will be managed by either the Head Teacher or another manager. If the matters are regarding the Head Teacher, then the Chair of Governors will be responsible for overseeing this Guidance.

What is Social Media?

For the purposes of this Guidance, the term social media is used to describe a type of interactive website or online tool that allows parties to communicate or interact with each other in some way by sharing information, opinions, knowledge and interests and to share data in a public forum or to participate in social networking, resulting in a number of different activities.

Social Media activities include, but are not limited to:

- Maintaining a profile page on social / business networking sites such as Facebook, Twitter, WhatsApp or LinkedIn
- Writing or commenting on a blog, whether it is your own or the blog of another person / informational site.
- Taking part in discussions on web forums or message boards such as YouTube.
- Leaving product or service reviews on business websites or customer review websites.
- Taking part in online polls.
- Uploading multimedia on networking sites such as You Tube, Instagram, WhatsApp Twitter and Tumblr.
- Liking, re-tweeting and commenting on posts of your own, another person or other social media account.

Many other forms of social media also exist which are not listed in this Guidance. Employees need to be aware that this is area is constantly changing and they are reminded of their continued responsibility to keep up to date with developments and review their privacy settings on a regular basis when using social media sites.

The Use of Social Media

The school recognises that employees will use social media in a personal capacity. However, it is important that employees understand that they are personally responsible for all comments, images or information that they post on line. Therefore, all employees must ensure that when posting any information, images or making comments, they do not:

- **Bring the School into disrepute**. E.g. by making derogatory or defamatory comments, either directly or indirectly, about the school, colleagues, individuals, pupils or parents etc that could negatively impact on the school's reputation or cause embarrassment. This includes posting images or links to inappropriate content or using inappropriate language.
- **Breach confidentiality**. E.g. revealing confidential information owned by the school relating to its activities, finances, employees or pupils.
- **Undertake any behaviour which may be considered discriminatory, or as bullying and/or harassment of any individual**. E.g. making offensive or derogatory comments (either directly or indirectly) relating to sex, gender, race, disability, sexual orientation, religion, belief or age; using social media to bully ("Cyberbullying") another individual; or posting images that are discriminatory or offensive or linking to such content.

As with all personal internet use, employees using social media sites must also observe the specific requirements of the documents named at the beginning of this policy.

Employee Responsibilities

Employees are personally responsible for the content that they publish on social media sites, including "Likes" (on Facebook)/"re-tweets" (on Twitter), Snapchat, Instagram, LinkedIn, Yammer, WhatsApp etc. Employees should assume that everything that is written is permanent and can be viewed by anyone at any time. It is fair and reasonable to take disciplinary action against employees for inappropriate use of social media, including use of social media conducted outside of working hours.

Employees must observe and note the following listed guidance (which is not exhaustive):

- Employees should assume that everything can be traced back to them personally as well as to their colleagues, the school, pupils and parents.
- To avoid any conflict of interest, employees must ensure that personal social networking sites are set to private, and pupils are never listed as approved contacts. An exception to this may be if the child is the employee's own child, relative, or family friend.
- Information must not be posted that would disclose the identity of pupils or could in any way be linked to a pupil(s). This includes photographs or videos of pupils or their homes.
- Pupils must not be discussed on social media sites.
- Employees should not post information on sites including photographs and videos that could bring the School [or the Local Authority] into disrepute.
- Employees must not represent their own views/opinions as being those of the school [or the Local Authority].
- Employees must not divulge any information that is confidential to the school [the Local Authority] or a partner organisation.

- Potentially false, derogatory, offensive or defamatory remarks directly or indirectly towards the School, [the Local Authority], employees, pupils, pupils' relatives, the school [or Local Authority] suppliers and partner organisations should not be posted on social media sites.
- Employees must ensure content or links to other content does not interfere with their work commitments or be on an inappropriate content.
- Employees must not either endorse or criticise service providers used by the school [or the Local Authority] or develop on-line relationships which create a conflict of interest.
- Employees must not upload, post, forward or post a link to any pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature).
- When posting on social media sites employees must observe the requirements of the Equality Act and the Human Rights Act and must not use any offensive, obscene, derogatory, discriminatory language which may also cause embarrassment to school the Local Authority, employees, pupils, pupils' relatives, Council suppliers and partner organisations.
- Employees must never impersonate another person.
- Employees must not upload~~,~~ forward or post a link which is likely to: create any liability for the School (whether criminal or civil), breach copyright law or other affect intellectual property rights, or which invades the privacy of any person.

Think before you post. There is no such thing as a private social media site. Social networking platforms/ Chat Rooms and discussion forums etc are in the public domain and it is not always possible to be sure what is being viewed, shared or archived, even if material is posted on a closed profile or group. There can be no reasonable expectation that posts will remain private and will not be passed on to other people, intentionally or otherwise.

Disciplinary Action

Employees should be aware that the use of social media sites in a manner contrary to this guidance, including if others implicate you in a breach of any of the points listed within this document may result in disciplinary action and in serious cases may be treated as gross misconduct, which itself could lead to summary dismissal.

In certain circumstances, such misuse may constitute a criminal offence or otherwise give rise to legal liability against employees and the school. Such cases will be referred to the police (and, where necessary the nominated safeguarding lead at the County Council) to investigate further.

Employees who become aware of any use of social media by other members of staff in breach of this guidance must to report the matter to the Head teacher.

Social Media Security

Employees should be mindful when placing information on social media sites that this information is visible to a large audience and could identify where they work and with whom, thereby increasing the opportunity for identify fraud, false allegations and threats. In addition, it may be possible through social media sites for children or vulnerable adults to be identified, which could have implications for their security. Employees should therefore be mindful that they:

- Do not reveal personal or private information about themselves such as date of birth, address details and bank details etc. Posting such information could increase the risk of identity theft. Remember that there is the scope for causing offence or unintentionally causing embarrassment, for example if pupils find photographs of their teacher which may cause embarrassment and/or damage to professional reputation and that of the School. Be mindful that posting images, comments or joining online campaigns may be viewed by colleagues, parents, ex-pupils etc. Ensure that where you do post comments make a clear statement that any comments expressed are your own and not those of the school [or Local Authority].

Finally, consideration should be given to the information posted on social media sites and employees are advised to use appropriately the security settings on such sites in order to assist in limiting the concerns above.

Monitoring the Use of Social Media Websites

Employees should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored and, where breaches of this Guidance are found, action may be taken under the Disciplinary policy.

The School considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media websites when he/she should be working; or
- acted in a way that is in breach of the rules set out in this Guidance

Heather Primary School Laptop Policy

Each class is assigned a School Laptop

Equipment Name	
Serial Number	
Staff member/members issued to	

The equipment shown above is issued by Heather Primary School to the member of staff indicated. The equipment is issued subject to the following conditions:

1. The equipment remains the property of Heather Primary School at all times and must be returned to the school at the end of the lease agreement or contractual period. The equipment nominated above is the sole responsibility of the named individual/s
2. Maintenance of the equipment is the responsibility of the School. All maintenance issues must be referred to the School office, through the usual channels.
3. From time to time, it will be necessary for the School to perform software updates and maintenance for which the equipment must be made available in school when requested – staff are responsible for ensuring they have made appropriate back-ups of their own school related data.
4. All installed software MUST be covered by a valid license agreement held by the school.
5. All software installation MUST be carried out by the School in accordance with the relevant license agreements.
6. When equipment is to be used to access the internet other than by the school broadband connection users MUST ensure that spyware protection software, anti-virus software and a firewall are installed. Connection to the internet should not be by wireless router, unless the wireless connection signal it is fully encrypted and password protected.
7. No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
8. Protective software must be updated regularly. For laptop computers, it will be necessary to connect them to the school network to update the antivirus software. This should be done regularly with updates continuously added automatically during normal in school use at least twice a weekly.
9. The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user.
10. All data storage devices such as flash drives/external hard dives must be encrypted
11. The School cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.
12. Internet usage is subject to the school E-Safety Policy and all adults in school are subject to the **Acceptable Usage Policy**.
13. If school equipment is to be used by anyone other than the member of staff responsible for it that user must have a separate account set up by the School. The laptop must remain in the user's possession at all times.
14. Equipment is insured by the LA whilst in school premises or the registered user's home. Whilst in transit it is only covered if it is in the possession of the user. If the equipment is in a situation where it is not covered by the LA insurance, users are responsible for organising their own insurance.

Name/s of recipients	
Recipient/s Signature	
Date of issue	

Device loan agreement for pupils

1. This agreement is between:

1) Heather Primary School ("the school")

2) [Name of parent and their address] ("the parent" and "I")

3) [Name of child] (the "pupil")

And governs the use and care of devices assigned to the parent's child. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil a laptop ("the equipment") for the purpose of doing schoolwork from home.

2. This agreement sets the conditions for taking a Heather Primary School laptop home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that myself and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Mrs. Davies in the school office, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Leave the device in a car or on show at home
- To not Eat or drink around the device
- To not to lend the device to siblings or friends
- To not Leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following taken from the acceptable use policy that I have previously signed for school:

"**To keep me safe whenever I use the internet or email, I promise…**

- to keep my username and password private and not to use anyone else's
- to keep all personal information private
- to block unknown links and attachments by not opening anything that I do not trust
- to report any messages or internet pages that are unsuitable or upsetting
- to tell someone I trust if someone asks to meet me offline

When using computer equipment ay home…

- I understand that my behaviour will be checked
- I will not play games unless I have permission
- I will not open, copy, delete or change anyone else's files, without their permission
- I will be polite and think carefully about how I talk to others online and what I say about them
- I will not take, copy or send pictures of anyone without their permission
- I will not try to upload, download or open any files, programmes or websites which are unsuitable or illegal
- I will not try to get around the filtering or security systems
- I will not install any programmes nor change the settings
- I will not use chat and social networking sites unless I have permission from an adult
- I will not copy other people's work and pretend it is my own
- I will not try to download pirate copies of music, videos, games or other software
- I will check that information I use from the internet is from a trusted website

If I break these rules…

- I understand that the school's behaviour guidelines will be followed"

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected making Make sure my child locks the equipment if it's left inactive for a period of time
- To not share the equipment among family or friends

If I need help doing any of the above, I will contact Mrs Davies on the email adminoffice@heather.leics.sch.uk

6. Return date

I will return the device in its original condition to the office within 5 school days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENT'S SIGNATURE	
LAPTOP SERIAL NUMBER, MAKE AND MODEL	