Maplewell Hall School

E-Safety Policy

Policy Created	**October 2016**
Governing Body Committee	
Date Reviewed by Governing Body	**H & S October 2016**
Date of Next Review	**October 2018**

Maplewell Hall School
E-safety policy

1. Introduction

1.1 Maplewell Hall School recognises the Internet and other digital technologies provide a good opportunity for children and young people to learn. These new technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2 As part of our commitment to learning and achievement we at Maplewell Hall School want to ensure that new technologies are used to:

- Raise standards.
- Develop the curriculum and make learning exciting and purposeful.
- Enable pupils to learn in a way that ensures their safety and security.
- Enhance and enrich their lives and understanding.

1.3 We are committed to an equitable learning experience for all pupils using ICT technology and we recognise that ICT can give disabled pupils increased access to the curriculum to enhance their learning.

1.4 We are committed to ensuring that **all** pupils will be able to use new technologies safely. We are also committed to ensuring that all those who work with children and young people, as well as their parents, are informed about the risks that exist so that they can take an active part in safeguarding children.

1.5 The nominated senior person for the implementation of the School's e-Safety policy is Meloney Ison, Assistant Head.

2. Scope of Policy

2.1 The policy applies to:

- all pupils;
- all teaching and support staff (including peripatetic), school governors and volunteers;
- all aspects of the School's facilities where they are used by voluntary, statutory or community organisations.

2.2 Maplewell Hall School will ensure that the following elements are in place as part of its safeguarding responsibilities to pupils:

- a list of authorised persons who have various responsibilities for E-safety;
- a range of policies including acceptable use policies that are frequently reviewed and updated;
- information to parents that highlights safe practice for children and young people when using new technologies;
- audit and training for all staff and volunteers;
- close supervision of pupils when using new technologies;
- education that is aimed at ensuring safe and responsible use of new technologies;
- a monitoring and reporting procedure for abuse and misuse.

3. Infrastructure and Technology

3.1 Partnership working

3.1.1 Maplewell Hall School recognises that as part of its safeguarding responsibilities there is a need to work in partnership. One of our major partners is the East Midlands Broadband Community (embc) who provide a managed (not 'locked down') network system. We fully support and will continue to work with embc to ensure that pupil and staff use of the Internet and digital technologies is safe and responsible.

3.1.2 As part of our wider safeguarding responsibilities, we seek to ensure that voluntary, statutory and community partners also regard the welfare of children as paramount. We therefore expect any organisation using the school's ICT or digital technologies to have appropriate safeguarding policies and procedures .

3.1.3 We work with our partners and other providers to ensure that any pupils who receive part of their education away from school are e-safe.

4. Policies and Procedures

Our policies are aimed at providing a balance between exploring the educational potential of new technologies and safeguarding pupils. We systematically review and develop our e-safety policies and procedures ensuring that they continue to have a positive impact on pupil's knowledge and understanding. We use the views of pupils and families to assist us in developing our e-safety policies and procedures.

4.1 Use of new technologies

4.1.1 We seek to ensure that new technologies are used effectively for their intended educational purpose, without infringing legal requirements or creating unnecessary risk.

4.1.2 Maplewell Hall School expects all staff and pupils to use the Internet, mobile and digital technologies responsibly and strictly according to the conditions below:[1] These expectations are also applicable to any voluntary, statutory and community organisations that make use of the school's ICT facilities and digital technologies.

Users 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.

4.1.3 Maplewell Hall 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

[1] For the purposes of this document, Internet usage means any connection to the Internet via web browsing, external email, news groups or messaging services, mobile technologies e.g. mobile phone, including Bluetooth applications, PDA's etc.

permission given by senior leaders, so that the action can be justified, if queries are raised later.

4.1.4 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.

4.1.5 <u>In addition, users are not allowed to:</u>

- Use the embc or an equivalent broadband provider's facilities for running a private business;
- Enter into any personal transaction that involves embc or member Local Authorities in any way;
- Visit sites that might be defamatory or incur liability on the part of embc or member Local Authorities or adversely impact on the image of embc;
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of embc, or to embc 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 embc
- Undertake activities with any of the following characteristics:
    - wasting staff effort or networked resources, including time on end systems accessible via the embc 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 embc 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 embc has requested that use cease because it is causing disruption to the correct functioning of embc;
    - other misuse of the embc 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.

4.1.6 Where Synetrix (provider of Internet connectivity and associated services to schools) and/or embc become aware of an illegal act or an attempted illegal act, they will comply with the law as it applies and take action directed by the police if a Regulation of Investigatory Powers Act (RIPA) Notice is issued.

4.2 Reporting Abuse

4.2.1 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 to the behavior manager or member of SLT. This information should be recorded via the behavior log, as well as, recorded in detail to ensure: -

- The website or email of inappropriate material is identified
- The filtering system is updated with the relevant detail
- Parent/carers are informed to raise their awareness of potential issues occurring online at home.

4.2.2 Maplewell Hall 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 LSCB[2] Procedures should be followed. The response of the School will be to take the reporting of such incidents seriously and where judged necessary, the Designated Senior Person for Child Protection within the School will 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 LSCB Procedures[3] assist and provide information and advice in support of child protection enquiries and criminal investigations.

Again any incident of this nature should be reported in full to a designated safeguarding lead, and this will be dealt with in accordance with the safeguarding policy.

5. Education and Training

5.1 Maplewell Hall School recognises that new technologies can transform learning; help to improve outcomes for children and young people and promote creativity.

5.2 As part of achieving this, we aim to create an accessible system, with information and services online, which support personalised learning and choice. However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use new technologies safely.

[2] Chapter 9 of the LSCB Procedures

[3] Chapters 5, 9, 12 and 13 of the LSCB Procedures

5.3 To this end we will:-

- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This will include teaching pupils to exercise the skills of critical awareness, digital literacy and good online citizenship.
- Audit the training needs of all school staff and provide training to improve their knowledge and expertise in the safe and appropriate use of new technologies.
- Work closely with families to help them ensure that their children use new technologies safely and responsibly both at home and school. We will also provide them with relevant information on our e-safety policies and procedures.
- Provide further learning opportunities within the 'Preparation for Adulthood' curriculum to engage pupils in current affairs in relation to e-safety and the potential risks due to their vulnerability.
- Ensure tutor teams are consistently applying the e-safety policy and usage to engage pupils in yet another learning opportunity.

6. Standards and Inspection

Maplewell Hall School recognises the need to regularly review policies and procedures in order to ensure that its practices are effective and that the risks to pupils are minimised.

Staff will receive updates with any concerns around e-safety during briefings, Inset sessions and via email. It is imperative that staff follow this guidance to ensure that pupils at Maplewell are protected.

6.1 Monitoring

6.1.1 Monitoring the safe use of new technologies includes both the personal use of the Internet and electronic mail and the monitoring of patterns and trends of use .

6.1.2 With regard to monitoring trends, within the school and individual use by school staff and pupils, Maplewell Hall School will audit the use of the Internet and electronic mail in order to ensure compliance with this policy. The monitoring practices of the school are influenced by a range of national and Local Authority guidance documents and will include the monitoring of content and resources.

6.1.3 We will also monitor the use of mobile technologies by pupils, particularly where these technologies may be used to cause harm to others, e.g. bullying (see anti-bullying policy for further information). We will also ensure that school staff understand the need to monitor our pupils, and where necessary, support individual pupils where they have been deliberately or inadvertently been subject to harm.

6.2 Reporting concerns

Any concerns regarding a pupil, member of staff, governor or visitor will be reported using the following guidance: -

- The observer to record the information seen, details of the content links, date and time and to hand directly to the Headteacher or member of SLT acting in this capacity at this moment. If a pupil is unable to record this they will need to give an account to an adult with this information.

- The observer to lock the screen, if possible, of the offending account. This enables any details to be kept current so that relevant links can be blocked through the filtering system.
- The Head teacher will follow details within the Staff conduct, Behaviour policy, Safeguarding and Whistle blowing policy to deal with the incident accordingly. The embc will be formed of the concerns to raise awareness of the issue identified.
- Information will be shared with any external professionals and the Head teacher will liaise with their direction.

Appendix 6 can be used to report the incident to support staff in doing so.

6.3 Sanctions

6.3.1 We will support pupils and staff as necessary in the event of a policy breach.

6.3.2 Where there is inappropriate or illegal use of new technologies, the following sanctions will be applied:

- *Child / Young Person*
  - The pupil will be disciplined according to the behaviour policy of the school.
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.
  - Pupils will potentially require access rights to be reviewed to ensure they are accessing appropriate content
  - The information will be discussed with parent/carers to ensure pupils are safe at home too
  - A pupil support intervention can be used to enable learning in further detail around the incident.

- *Adult (Staff and Volunteers)*
  - The adult may be subject to the disciplinary process, if it is deemed he/she has breached the policy
  - Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for example, illegal Internet use or child protection concerns.

6.3.2 If inappropriate material is accessed, users are required to immediately report this to a member of SLT and embc so this can be taken into account for monitoring purposes.

7. Working in Partnership with Parents/Carers and professionals

7.1 We are committed to working in partnership with parents and carers and understand the key role they play in maintaining the safety of their children, through promoting Internet safety at home and elsewhere.

7.2 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.

7.3 Maplewell Hall maintains close contact with any partnership to enable support for individual pupils to be put into place

7.4 Maplewell Hall will share updates and information with our partnerships to ensure pupil safety is paramount

7.5 Maplewell Hall will endeavor to enable parenting sessions that highlight concerns around e-safety and the risks pupils with SEN may face

8. Other relevant policies and procedures

- Acceptable use policy for pupils
- Acceptable use policy for staff
- Safeguarding policy
- Behaviour policy
- ICT audit assessment grid
- Privacy and data protection notices.

Appendix 1- Acceptable use ‘pupil friendly’ agreement

Acceptable Use Policy for pupils at
Maplewell Hall School

ZIP IT
Keep your personal stuff private and think about what you say and do online.
BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.
FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

- I will not share my username and password or try to use anyone else’s
- I will not post online any personal information about myself or others
- I will block attachments to emails by not opening anything sent that I do not trust or recognise – it may contain a virus
- I will immediately report any messages or internet content that is inappropriate or makes me feel uncomfortable
- I will immediately report any damage or faults involving equipment or software

- I understand that the school will monitor my use of school computer equipment and the internet
- I will not use the school ICT systems for personal or recreational use unless I have permission to do so
- I will respect other people’s work and property and will not access, copy, remove or otherwise alter anyone else’s files, without their permission
- I will be polite and responsible when I communicate with others online
- I will not take or distribute images of anyone without their permission
- I will only use my mobile phone and other handheld devices in accordance with the school policy
- I will not try to upload, download or access any materials which are illegal or inappropriate
- I will not use any way of trying to bypass the filtering / security systems, designed to prevent access to inappropriate material
- I will not try to install any programmes on a school computer nor alter the settings
- I will only use chat and social networking sites with permission and at the times that are allowed, in accordance with the school policy
- I will respect the copyright of others in my own work
- I will not try to download pirate copies of music, videos, games or other software
- I will take care to check that information I use is accurate
- I understand that if I break this agreement, the school will take action according to the school behaviour guidelines
- I understand that Police could be involved if something I did was illegal

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 ______________

Appendix 2- Letter for parent/carers

Dear Parent/Carer,

Use of Internet and e-mail in school

As part of their work in Information Technology and other subjects, we offer the children supervised access to the Internet and **internal** e-mail. On some occasions children are offered the opportunity to use e-mail outside the school, for example to communicate with children from other schools.

The Internet is a rich source of information and educational activities which are of great benefit to the children. However there are concerns about inappropriate materials and the school takes a range of measures to minimise these risks:

- All access to the Internet is supervised by adults
- A high level filtering system is in operation.
- Children are not allowed access to social media sites at any time
- Children are taught about safe Internet use by their teachers

Before we allow children to use the Internet at school, we must obtain parental permission. If you are happy to allow your child to access the Internet, please complete the enclosed form and return it to school.
Pupils and parents **must** sign and return the Internet Use Permission Form below as evidence of their acceptance of the school's rules for responsible use of these facilities before their child is allowed access.

Yours sincerely,

Headteacher

I have read the notes about Internet access at school and I have discussed them with my child.

I agree for my child _____________________________ Class __________

to use the Internet in accordance with the school guidelines.

Signed _______________________________________ Parent/Carer

Signed _______________________________________Pupil

Date: ____________________

Appendix 3-Maplewell Hall School

Staff Laptop Policy (this policy covers all mobile digital equipment)

Equipment Name.	
Serial Number.	
Issued to Staff Member.	

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

1. The equipment remains the property of Maplewell Hall School at all times and must be returned to the college at the end of the lease agreement or contractual period. The equipment nominated above is the sole responsibility of the named individual.

2. Maintenance of the equipment is the responsibility of the ICT support department. All maintenance issues must be referred to the ICT support department, through the usual channels.

3. From time to time, it will be necessary for the ICT support department to perform software updates and maintenance for which the equipment must be made available in college when requested.

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 ICT support department 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. It is strongly recommended that all data is regularly backed up, either to a CDRW disk, a memory stick or to the school network.

10. The ICT support department cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

11. Internet usage is subject to the school e-Safety Policy.

12. School equipment should not be used to access any web-based e-mails apart from the EMBC Portal and the school VLE, as the ICT support department is unable to offer any guarantees regarding the availability, performance, reliability or safety of such services.

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 ICT Support Department. The laptop must remain in the users possession at all times.

14. Equipment is insured by the LA whilst in school premises or the registered users 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 of recipient

Recipient's Signature

Date of Issue ____________________

Appendix 4- School website policy (to be published on the website)

The School operates the following policy on its website regarding the use of photographs, to ensure the privacy and safety of pupils at the school:

1. Where pupils are named, only their first names are given;
2. Where a pupil is named, no photograph of that pupil is displayed;
3. Where a photograph is used which shows a pupil, no name is displayed.

By observing these points, the school ensures that visitors to the website cannot link images of pupils to names of pupils.

The school follows a policy of seeking parents' permission before using images which show pupils on the website.

No other private information about pupils is ever published on the website such as surnames or contact details.

Website Privacy Policy

We are committed to safeguarding the privacy of our website visitors; this policy sets out how we will treat your personal information.

(1) What information do we collect?

We may collect, store and use the following kinds of personal data:

1. Information about your visits to and use of this website;
2. Information about any transactions carried out between you and us on or in relation to this website;
3. Information that you provide to us for the purpose of registering with us, and/or leaving guestbook comments, and/or subscribing to our website services and/or email notifications.

(2) Information about website visits

We may collect information about your computer and your visits to this website such as your IP address, geographical location, browser type, referral source, length of visit and number of page views. We may use this information in the administration of this website, to improve the website's usability, and for marketing purposes.

We use cookies on this website. A cookie is a text file sent by a web server to a web browser, and stored by the browser. The text file is then sent back to the server each time the browser requests a page from the server. This enables the web server to identify and track the web browser.

We may send a cookie which may be stored by your browser on your computer's hard drive. We may use the information we obtain from the cookie in the administration of this website, to improve the website's usability and for marketing purposes. We may also use that information to recognise your computer when you visit our website, and to personalise our website for you.

Most browsers allow you to refuse cookies. (For example, in Internet Explorer you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector.) This will, however, have a negative impact upon the usability of many websites.

(3) Using your personal data

Personal data submitted to this website will be used for the purposes specified in this privacy policy or in relevant parts of the website. In addition to the uses identified elsewhere in this privacy policy, we may use your personal information to:

1. Improve your browsing experience by personalising the website;
2. Provide other organisations with statistical information about our users - but this information will not be used to identify any individual user.

We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing.

(4) Other disclosures

In addition to the disclosures reasonably necessary for the purposes identified elsewhere in this privacy policy, we may disclose information about you:

1. To the extent that we are required to do so by law;
2. In connection with any legal proceedings or prospective legal proceedings;
3. In order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk);
4. Except as provided in this privacy policy, we will not provide your information to third parties.

(5) Security of your personal data

We will take reasonable precautions to prevent the loss, misuse or alteration of your personal information. Of course, data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

(6) Policy amendments

We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

(7) Third party websites

The website contains links to other websites. We are not responsible for the privacy policies of third party websites.

(8) Our contact details

Please see above for our contact details.

Website Disclaimer

(1) Introduction

This disclaimer governs your use of our website; by using our website, you accept this disclaimer in full. If you disagree with any part of this disclaimer, do not use our website.

(2) Intellectual property rights

Unless otherwise stated, we or our licensors own the intellectual property rights in the website and material on the website. Subject to the licence below, all our intellectual property rights are reserved.

(3) Licence to use website

You may view, download for caching purposes only, and print pages from the website, provided that:

1. You must not republish material from this website (including republication on another website), or reproduce or store material from this website in any public or private electronic retrieval system;
2. You must not reproduce, duplicate, copy, sell, resell, visit, or otherwise exploit our website or material on our website for a commercial purpose, without our express written consent.

(4) Limitations of liability

The information on this website is provided free-of-charge, and you acknowledge that it would be unreasonable to hold us liable in respect of this website and the information on this website.

Whilst we endeavor to ensure that the information on this website is correct, we do not warrant its completeness or accuracy; nor do we not commit to ensuring that the website remains available or that the material on this website is kept up-to-date.

To the maximum extent permitted by applicable law we exclude all representations, warranties and conditions (including, without limitation, the conditions implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill).

Our liability is limited and excluded to the maximum extent permitted under applicable law. We will not be liable for any direct, indirect or consequential loss or damage arising under this disclaimer or in connection with our website, whether arising in tort, contract, or otherwise - including, without limitation, any loss of profit, contracts, business, goodwill, reputation, data, income, revenue or anticipated savings.

However, nothing in this disclaimer shall exclude or limit our liability for fraud, for death or personal injury caused by our negligence, or for any other liability which cannot be excluded or limited under applicable law.

(5) Variation

We may revise this disclaimer from time-to-time. Please check this page regularly to ensure you are familiar with the current version.

(6) Entire agreement

This disclaimer constitutes the entire agreement between you and us in relation to your use of our website, and supersedes all previous agreements in respect of your use of this website.

(7) Law and jurisdiction

This notice will be governed by and construed in accordance with English law, and any disputes relating to this notice shall be subject to the exclusive jurisdiction of the courts of England.

(8) Our contact details

Please see above for our contact details.

Appendix 5-

E-safety Checklist for Maplewell Hall School

Policies, practice and monitoring	Yes	No	Action/evidence
Does the school have an e-safety policy in place?	Y		E-safety policy revised Oct 2016
Are there ‘Acceptable Use Policies’ for both pupils and adults?	Y		Policies in place for staff and pupils
Is cyber bullying addressed in the school’s anti-bullying policy?	Y		Positive Behaviour for learning policy
Are there effective sanctions in place for breaching the policy?	Y		Positive Behaviour for learning policy E-safety policy
Has the school appointed an e-safety co-ordinator?	Y		Meloney Ison, Assistant Head
Is e-safety provision rigorously and regularly reviewed?	Y		Pupil behaviour log Cause for concern slips SLT minutes
Does the school keep a log of e-safety incidents and alter provision if necessary?	Y		Pupil behaviour log Emailed action points
Has an evaluative comment on e-safety been included in the SEF?	Y		Ensure the area is continuously monitored and improving

Infrastructure	Yes	No	Action
Is the school network safe and secure?	Y		ICT technician maintains regular checks on the system
Does the school use an accredited internet service provider? *Eg embc*	Y		Embc used
Does the school use internet filtering/monitoring?	Y		Capita used Current consideration of a new provider being investigated
If there are changes made to the internet filtering setup are these authorised by a senior manager?	Y		SLT liaise with ICT technician to monitor the filtering system
Learners	**Yes**	**No**	**Action**
Do learners understand what safe and responsible online behaviour means and do they use it?	Y		All staff ensure this message is constantly reinforced during lessons with the e-safety and behaviour policy in mind
Is e-safety education a regular part of the curriculum?	Y		All pupils have a ICT lesson All pupils have 'Preparation for adulthood'
Do learners know and understand the UKCCIS digital code –	Y		This is included with the pupil agreement for ICT usage
Do learners know how to report e-safety concerns they may have? *Eg CEOP Report Abuse button, reporting to an adult in school*	Y		Regular assemblies Embedded knowledge during ICT lessons
Staff	**Yes**	**No**	**Action**
Do teaching staff understand e-safety issues and risks?	Y		Staff are vigilant at reporting any issues or concerns to SLT Regular Inset and safety updates provided to staff
Have they received training which is regularly updated?	Y		CPD system Induction process
Do staff know who to report to with an issue of concern regarding e-safety?	Y		Any concerns to be reported to SLT as per the e-safety policy
Do they keep data safe and secure? Eg encrypted personal assessment data, use of password protection	Y		Emails include pupil initials AVCO used for transferring data to LCC Password protection and encryption used for sensitive material
Do they take measures to protect themselves online? *Eg keep personal information private, use secure passwords*	Y		SIMS passwords prompt for updated password Screen lockdowns on equipment

Do they conduct themselves professionally online? *Eg social networking sites, blogs*	Y		Staff consistently send a positive outwards message as per the safer recruitment policy
Parents / Governors	**Yes**	**No**	**Action**
Do governors have a general understanding of the issues and risks associated with e-safety?	Y		Concerns presented to Head of governors who is the safeguarding link H&S meetings held each term
Does the school keep parents aware of e-safety issues through eg newsletters, leaflets, open assemblies, updates etc?	Y		Parent groups arranged by HSLW Newsletter updates Letters outlining concerns Telephone calls
Has the school held an e-safety Parent Awareness Session?	Y		During parents evening

Appendix 6- E-Safety Incident Record

Use this form to record the details of serious e-safety incidents and the action taken. Hand to Meloney Ison(e-safety co-ordinator) for monitoring purposes.

E-safety incident						
Name of staff member discovering			**Date**:		**Time**:	
Name of pupils / staff involved						
Nature of incident (tick box)	Failing to report accidental access to inappropriate material	Intentional access to inappropriate material	Cyber Bullying	Grooming	Other	
Details						
When incident occurred (tick)	During a lesson	Outside lesson time	Outside school			
Is police involvement needed? (Yes if…)	Grooming	Indecent images of children	Criminally obscene material	Criminally racist or discriminatory	Violent / bomb making	Other criminal conduct
Signed by Head Teacher			Date:		Time:	
STAFF **Action taken eg HR contact, Chair of Governors, disciplinary action, police**						
PUPIL **Action taken eg Contact parents, sanction applied, police**						

Appendix 7- E-Safety Standards for Leicestershire Schools

Maplewell Hall School

Date of review 1st October 2016

Name of reviewer/s Meloney Ison

E-safety Standard	Target Aspects	Where are we now?	Next Steps Action
Children and young people are safe and feel safe when using the internet	• Children and young people say they feel safe in school when using online technologies and understand the importance of this. • E-safety policies and procedures are in place to keep children and young people safe.	Pupils currently completing a perception survey via survey monkey E-safety and safeguarding policy up-to-date	Use pupil data to compile improvements around 'feeling safe in school' to ensure MHS is outstanding in this area RC
All users understand the online risks they face and know how to minimize these	• Children are taught about different online risks they face and know to keep personal information private, how to respond to challenges to their safety and when to report their concerns. • All adults in school are well informed about e-safety, report incidents and respond appropriately.	Informed ICT lessons Preparation for adulthood curriculum Acceptable use policy for staff and pupils	Termly Inset to highlight any areas of concerns Rigorous measures with the filtering system to be enforced
There are appropriate safeguards built into the technology infrastructure	• There is a filtering infrastructure for all users that is well-managed, age appropriate and role specific.* • Where there is local control of filtering, senior managers have clear accountability.	ICT technician manages the filtering infrastructure of the school with Capita SLT liaise with technician regarding any concerns	Research different providers to ensure safety standards are always high and maintained- AP/AHa Complete the following audit http://www.nen.gov.uk/school-e-security-checklist/ Ap/AHa
Links between parents, governors, teachers, learners and other stakeholders effectively support a secure e-safety environment	• The governor responsible for safeguarding has effective oversight of the e-safety culture of the school and has strong links with the e-safety co-ordinator. • Parents are well-informed about e-safety through awareness raising activities and by countersigning an Acceptable Use Policy. • Parents are informed of serious e-safety incidents involving their own children and are contacted where serious breaches of the Acceptable Use Policy have occurred.	H&S meetings flag concerns and actions Parent/carers are informed directly, via meetings, parents evening, newsletter, parent sessions Any serious matters are communicated via face-to-face meetings	Continue monitoring at this standard and providing update sessions to ensure all partnerships are aware of current trends
The online behaviour of all staff and learners demonstrates an outstanding appreciation of e-safety issues	• All staff and learners set strong passwords and keep them private. • Staff members do not make private online contact with pupils nor accept pupils or parents as 'friends' on social networking sites. • All online communication and internet use by staff in school is professional and all personal data is kept secure. • Staff and learners understand the importance of "ThinkB4UPost" and all online communication is respectful and polite. • The e-safety code "Zip-it, Block-it, Flag-it" (or equivalent) is understood and applied by all users.	Every user on site has a unique login name and password All social networking sites are blocked through the filtering system All data is kept secure and sent via the appropriate channels All emails are monitored to ensure a high professional standard at all times Pupil usage agreement	Continue developing the knowledge of learners to understand e-safety issues
School policies and procedures are	• Acceptable Use Policies are reviewed regularly and have been signed by all staff and pupils and counter-signed by parents.	Acceptable use policies in place and followed	Ensure all agreements signed and on file- AP/HA

followed by all users and regularly reviewed and updated	• The e-safety policy is followed by everyone and reviewed regularly. • New staff receive an induction on the acceptable use of ICT which includes e-safety. • E-safety is referenced in other school policies eg behaviour, anti-bullying (cyber-bullying), PSHE etc. • E-safety is evaluated and evidenced effectively.	Signed copies kept on file Monitoring and review of the policy constantly in-place Induction process inset E-safety is referenced throughout all policies E-safety is continuously reviewed and monitored to ensure high safety expectations	Inset as required- MI
E-safety education is fully embedded within the wider school curriculum and teaching and learning is rigorously monitored, evaluated and adapted to improve e-safety	• There is an age-appropriate e-safety curriculum which is structured, progressive and visited regularly across different subjects including PSHE. • It is monitored by a subject leader, adapted and kept up to date in line with changes in new technology. • Lessons are evaluated and adapted to take account of e-safety incidents.	All pupils access ‘Preparation for Adulthood’ that covers aspects of online behaviours, vulnerability, understanding how to stay safe. The ICT curriculum covers information regarding safety continuously and update as required Monitored by DL/RC	Continuously improve and develop the curriculum
Learning from e-safety incidents is used to impact positively on student safety	• There is a log of e-safety incidents that is regularly reviewed by senior managers and used to adapt the curriculum and revise policies. • Monitoring identifies breaches of the Acceptable Use Policy which are followed up with the individual concerned. • Disciplinary and Safeguarding procedures are followed where appropriate. • Where cyber bullying has been identified, perpetrators are required to remove abusive content from profiles / blogs / websites etc and serious incidents are reported to the Police as appropriate.	E-safety incidents recorded on SIMS and reviewed during SLT meetings. Any breaches followed up via the behaviour policy Safeguarding policy in place Cyberbullying is documented and reported to the necessary persons	Continually monitor and implement the relevant policies and procedures
All staff receive e-safety training which makes an outstanding impact on outcomes	• All teaching staff (including Learning Support Assistants) receive e-safety training which is updated to include new developments in technology.	E-safety training forms part of termly updates ICT training provided to support LSAs	Continually develop CPD opportunities for staff
Rigorous self-assessment includes listening to the voice of children and young people and leads to evidence based decisions having a very positive impact	• The e-safety co-ordinator or group oversees a regular review of e-safety* including feedback from incident monitoring. • Children and young people are consulted on e-safety through pupil surveys and school council meetings.	SLT meeting notes and follow-up actions completed All information logged on SIMS Pupils to complete perception and safety surveys termly via survey monkey	Continuous review of the e-safety policy and procedures to ensure pupils feel safe

Appendix 8- Incidents around Facebook

What can schools do when an incident on Facebook arises?

1. If you know the identity of the perpetrator contacting their parents or, in the case of older children, the young person themselves to ask that the offending content be removed often works.
2. Failing that, having kept a copy of the page or message in question delete the content.

- For messages the delete and report / block user facilities are found in the 'Actions' dropdown on the page on which the message appears.
- For whole pages the unfriend and report / block user facilities are at the bottom of the left hand column. Always try to cite which of the Terms and Conditions (See footnote for the most likely ones[1]) http://www.facebook.com/terms.php or Community Standards http://www.facebook.com/communitystandards/ have been violated because Facebook are more alert to US law than UK. The process should be anonymous.
- If the page is by someone under 13 click on: http://www.facebook.com/help/contact.php?show_form=underage Facebook say they will delete any such page.
- To remove a post from a profile, hover over it and on the right there will be a cross to delete it.

3. Does the incident trigger the need to inform the police or child protection agencies?
4. To report abuse or harassment email abuse@facebook.com (Facebook will acknowledge receipt of you email and start looking into your complaint within 24 hours. They will get back to you within 72 hours of receiving your complaint.)
5. If all else fails support the victim, if they wish, to click the 'Click CEOP' button at http://www.thinkuknow.co.uk/ or www.ceop.police.uk (This will provide access to a range of support services. In addition this enables them to report directly to CEOP if someone has acted inappropriately towards a child or young person online. This may be sexual chat, being asked to do something that makes them feel uncomfortable or someone being insistent on meeting up.)
6. If the victim is determined to continue using Facebook they might want to delete their account and start again under a different name. Deletion can be done here https://ssl.facebook.com/help/contact.php?show_form=delete_account They should be made aware of the privacy issues that might have given rise to their problem in the first place.

An effective education programme can help to reduce the number of times that this sort of incident arises, over the medium term. Such a programme should help young people to match their online behaviour with their offline behaviour by helping them to develop understanding, skills and behaviours in these sorts of areas:

- possible consequences
- understanding the effects of bullying on others
- understanding how technology can magnify impact
- understanding how comments or other actions can be perceived differently by the originator and the target

Appendix 9- Useful websites

http://www.emergingedtech.com/2014/06/10-proactive-steps-to-reduce-social-media-issues-for-young-students-in-your-schools/ Ten issues of concern around social media

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf This document provides information around concerns relating to radicalisation and the Prevent duty

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf Specific government advice regarding the Prevent Duty

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf Government advice regarding cyberbullying

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/547327/Inspecting_safeguarding_in_early_years_education_and_skills_settings.pdf Inspecting safeguarding in schools

http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals a range of resources to support educational topics

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/ advice for parent/carers regarding keeping children safe online

https://www.thinkuknow.co.uk/parents/ further advice for parent/carers

https://www.ceop.police.uk/safety-centre/Parents/ This link highlights how to report abuse online

https://leics.police.uk/categories/cease Information supplied by Leicestershire Police regarding the ‘CEASE’ pledge