e-Safety and Social Media Policy

Legislation

Settings are advised to risk assess social media tools to comply with The Health & Safety at Work Act 1974, The Children Act 1989, The Childcare Act 2006, The Management of Health and Safety at Work Regulations 1999 and The Computer Misuse Act 1990 which clarify that all settings have a duty of care to ensure the safety and wellbeing of children and staff.

Additional: The Statutory Framework for the Early Years Foundation Stage pg.14, 3.6 states; 'training made available by the provider must enable staff to identify signs of possible abuse and neglect at the earliest opportunity and to respond in a timely and appropriate way. Providers must train all staff to understand their safeguarding policy and procedures which should include inappropriate behaviour displayed by other members of staff which includes the inappropriate sharing of images'.

1.0 e-Safety Policy

1.1 Aim

To ensure staff/early year's practitioners have a clear and agreed understanding of the benefits and risks of e-safety. It will provide advice on acceptable use and effective control measures to enable individuals to use ICT resources in a safe online environment.

- Safeguarding children is everyone's responsibility so it is of paramount importance to ensure the safety and wellbeing of children at all times and this includes their online safety.
- The registered person will have the overall legal, personal and moral responsibility to ensure that online safety is effectively considered.
- The designated person for safeguarding is to be responsible for online safety alongside the administrator for social media, and will manage the implementation, monitoring and reviewing of the e-safety policy.

To minimise any risks all staff should have effective training on e-safety. A reliable infrastructure and a clear Acceptable Use Agreement (AUA) should be in place which is key to effective practice (Appendix 1).

Creating a safer online environment will be on-going, so clear monitoring, evaluation and review of procedures are essential.

All staff should support children's emerging understanding of e-safety by providing a range of resources to support their learning including cameras, ipads, tablets, computers and any other android devices as is appropriate or available.

Staff should be committed to acknowledge and assess risks to create a balanced approach. Relevant documentation such as incidents logs (Appendix 5) and written risk assessments must be completed in accordance with the acceptable use policy (AUP).

1.2 Settings Social Media Policy and Procedure

Social media tools can provide excellent opportunities for teaching and learning, however such sites can have risks and can never be 100% safe. These risks can be minimised by having an embedded e-safety policy and individuals should consider having separate personal and business on-line communication tools.

1.3 Administration & Monitoring

Staff must be aware of their personal and professional conduct when using social media. Staff using social media should consider what information is published to ensure confidentiality is observed at all times and the setting is not brought into disrepute. Content can be easily shared online and circulated far and wide without consent or knowledge, possibly resulting in disciplinary, civil or criminal consequences.

1.4 Ethical Considerations

As a communication tool user you should consider the potential associated dangers of posting images, photographs and information on social networking sites.

Key safety concerns include:

- Children being easily identified by their image posing a risk of inappropriate contact by individuals (children's names must not be displayed alongside their images)
- Images being altered and distorted
- Images being used inappropriately causing stress and anxiety

All individuals regardless of age should have a right to participate in the decision making of how information is used and published. The views of children must be considered to comply with 'United Nations Convention on the Rights of the Child':

- Article 3: Best interests of the child
- Article 12: Respect for the views of the child
- Article 13: Freedom of expression
- Article 16: Right to privacy

For further information regarding the law refer to Staffordshire Safeguarding Children Board website: - www.staffsscb.org.uk

The potential risks and use considerations need to be balanced alongside the many benefits of sharing information electronically. These include parents more readily accessing information regarding the setting that their child attends and children being excited about seeing photographs of themselves displayed on the web, bringing the page to life.

2.0 Exemplars

2.1 Appendix 1

Staff Acceptable Use Policy – see policy folder

2.2 Appendix 2

e-Safety Parental Permission Form

Dear Parent/Carer

As part of the programme of activities to support your child's learning and development, they will have the opportunity to access a wide range of information and communication technology (ICT) resources.

We recognise the important contribution and value that such resources have in promoting children's learning and development, however, we also recognise there are potential risks involved and therefore have robust e-safety policies and procedures in place.

Please read and sign the permission form below.

Should you wish to discuss the matter further please do not hesitate to contact me.

Yours sincerely,

(Manager)

Parent/Carer e-Safety Permission Form

I give permission for my child to access digital technologies in accordance with Mercia Primary Academy Trust e-safety policies and procedures.

Child's Name: _____

Parent/Carer Name: _____

Parent/Carer Signature: _____ (person with parental responsibility)

Date: ___/___/___

2.3 Appendix 3

Staff Conduct Agreement

We acknowledge that practitioners will use digital technologies in their personal and social lives so we require them to sign the following Professional Conduct Agreement to ensure clear boundaries between their home and professional roles.

I agree that through my recreational use of social networking sites or other online technologies that I will:

- not bring Mercia Primary Academy Trust into disrepute;
- observe confidentiality and refrain from discussing any issues relating to work;
- not share or post in an open forum, any information that I would not want children, parents/carers or colleagues to view;
- set privacy settings to block unauthorised access to my social networking page and to restrict those who are able to receive updates;
- keep my professional and personal life separate and not accept children and parents/carers as 'friends';
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of the Mercia Primary Academy Trust;
- either avoid using a profile photograph or ensure it is an image I would be happy to share with anyone;
- report any known breaches of the above;

I understand I am in a position of trust and my actions outside of my professional environment could be misinterpreted by others, and I am conscious of this when sharing information publicly with others.

Name: _____ Signature: _____

Date: ___/___/___

2.4 Appendix 4

Setting's Social Media Conduct Agreement

We require you to sign and agree to follow the Conduct Agreement for using Mercia Primary Academy Trust t social media communication platforms to ensure clear boundaries between and Mercia Primary Academy Trust home are followed.

Social Media platform: _____

I agree to:

- not bring Mercia Primary Academy Trust into disrepute by following their social media policy;
- observe confidentiality by not discussing other children, parents or practitioners;
- not share, tag, post or copy any information from Mercia Primary Academy Trust social media platform without prior permission from the 'management';
- keep my professional and personal life separate and not accept children/ parents/carers as 'friends' on my personal page;
- consider how my social conduct may be perceived by others and how this could affect my own reputation and that of Mercia Primary Academy Trust;
- report any known breaches of the above to the designated person for safeguarding Mercia Primary Academy Trust and named social media administrator for social media;
- I understand I am in a position of trust and my actions could be misinterpreted by others and I am conscious of this when sharing information with others on the social media platform site belonging to Mercia Primary Academy Trust.

Name : _____ Signature: _____

Date: ____/____/____

2.5 Appendix 5

Online Incident Log Sheet

An e-safety flow chart to assist you in determining the process to follow in the event of an e-safety incident refer to www.safenetwork.org.uk

To be completed as thoroughly as possible by the practitioner or manager identifying incident

Date(s) / time(s) of incident:
Duration of incident: (e.g. one off, a week
Description of the online safety incident (include details of specific services or websites used e.g. chat room, email addresses, usernames etc.
Why do you have concerns about this incident?
Has the information been recorded and secured? Yes/ No
Has any computer or hardware been secured? Yes/ No
If yes, give details including who, where, when and what?

Who was involved and how do you know this?
Is there any evidence to suggest that false names/details have been given? (Give full details of real names and email addresses where known).
How was the incident identified? e.g. by member of staff

What actions were taken, by whom and why? (Give detail of agencies informed and contact person within those agencies).
Name of person completing this form:
Position:
Name of setting:
Signature:
Date:

2.6 Appendix 6

e-Safety Audit

This self-audit should be completed by the Manager, the designated person for safeguarding and the designated person for monitoring any online communication tools.

Staff, parents and carers could also contribute to this audit tool.

Date of e-safety policy update:
Date of future review:
The e-safety policy was agreed by the senior management team on:
The registered person is:
The Safeguarding Coordinator is:
The e-safety Coordinator is:

Task	**Yes/No**	**Comments**
Does the e-safety policy comply with local safeguarding children board's e-safety procedures and guidance?		
Is e-safety included in the induction process for all new staff?		
Has up to date training been provided for all individuals?		
Are all individuals (staff, parents, carers and any volunteers) familiar with the e-safety policy and the Acceptable Use Policy?		
Are all individuals (staff, parents, carers and any volunteers) familiar with the e-safety policy and the Acceptable Use Policy?		
Have staff and any volunteers (including parents / carers if applicable) signed a disclaimer to say they have read and understand the e-safety Policy and the Acceptable Use Policy?		
Have parents/carers returned and signed a copy of the e-safety parental permission		

form?		
All individuals are compliant with additional AUP's (social media sites, learning platforms) and have signed the additional disclaimer for their use.		
Do users understand the use of e-safety monitoring software (if applicable)?		
Did you consult staff, Parents/carers when updating the e-safety policy?		
Are all individuals made aware of the settings expectation around safe and professional online behaviour?		
Is there a clear procedure for all individuals to follow when responding or reporting an e-safety incident or concern?		
Is personal data collected, stored and used in accordance with the principles of the Data Protection Act and ICO?		
Have you accessed and distributed e-safety materials from SSCB, CEOP, Childnet and UKCCIS?		
Have you devised an e-safety and social media incident log that is used to record incidents and any action taken?		
Have you devised e-safety and social media rules? How are these communicated to individuals?		

3.0 References and Contacts for e-safety and Social Media

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
Childline: www.childline.org.uk
Childnet: www.childnet.com
Connect Safely: http://www.connectsafely.org/
Cybermentors: www.cybermentors.org.uk
Digizen: http://www.digizen.org/
Facebook Safety Centre: https://en-gb.facebook.com/safety/

Information Commissioner's Office - Data Protection:
http://www.ico.org.uk/for_organisations/data_protection

Internet Watch Foundation (IWF): www.iwf.org.uk
Kent e–Safety in Schools Guidance: www.kenttrustweb.org.uk?esafety
Kidsmart: www.kidsmart.org.uk
Safe Network- http://www.safenetwork.org.uk/

Staffordshire Safeguarding Children Board: http://www.staffsscb.org.uk

South West Grid for Learning Online Safety: http://www.swgfl.org.uk/Staying-Safe

Teach Today: http://en.teachtoday.eu
Think U Know website: www.thinkuknow.co.uk
Twitter- Safety Tips for Parents: http://support.twitter.com/articles/470968-safety-tips-for-parents#
Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com
Wired Safety - https://www.wiredsafety.org

Signed ……

Director, Mercia Primary Academy Trust

Disclaimer