Curzon Crescent & Fawood Children's Centres Partnership

E-Safety Policy

Adopted Brent Council
Digital Safety/Social Media and Acceptable Use

Policy Lead:
Business Manager

Approving Committee:
Resources

Adopted: Summer 2019

Review: Summer 2021

Contents Page

1. Introduction

Computing and the use of devices is seen as an essential resource to support teachers and actual learning; as well as playing an important role in the everyday lives of children, young people and adults. The widespread availability and use of digital devices and social media applications brings opportunities to understand, engage, and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our school, our children's centres, the community, our legal responsibilities and our reputation. For example, our use of social networking applications has implications for our duty to safeguard children and young people.

Information and Communication Technology (ICT) covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole.

This policy applies to the governing board, all teaching and other staff, whether employed directly or indirectly by the Partnership, external contractors providing services, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the Partnership. These individuals are collectively referred to in this policy as Staff.

This policy provides a good practice approach to using the internet and social media and will ensure that the use of social media is effective, lawful and does not compromise the Partnership's reputation, school and children's centre information or computer systems/networks.

2. Purpose

The purpose of the policy is to:

- ensure staff use digital devices and social media responsibly, to avoid bringing the Partnership into disrepute
- safeguard all children and staff
- ensure that where information is provided through social media regarding the Partnership, it is representative of our ethos and the work we do

3. Roles and responsibilities

The governing board will ensure that this policy will reviewed and monitored as appropriate.

The Executive Headteacher will ensure that the School has a nominated E-Safety Lead (ESL) tasked with overseeing and managing the recording, investigation and resolution of digital safety incidents. Contact details for the

school's ESL is attached as Appendix 2 to this policy. The nominated ESL will be suitably trained in order to undertake this role. The Executive Headteacher and Senior Leadership Team will familiarise themselves with government guidance on digital safety and in particular the prevention of bullying (see website: https://www.gov.uk/government/publications/preventing-and-tackling-bullying).

All staff will familiarise themselves with this policy and will be provided with relevant information, guidance and training in digital safety insofar as is appropriate to the discharge of their duties. All staff and governors are expected to read and sign the declaration attached at Appendix 3 to confirm they have read and understood the E-Safety Policy (covering Digital Safety/Social Media and Acceptable Use).

4. Definitions

Social media is a collection of on-line communication channels that allow people to create, share or exchange information, conversations, pictures and videos.

Social networking applications can include Facebook and Twitter, Instagram, Snapchat, messaging on MSN and on mobile phones, blogs, LinkedIn, online discussion forums, YouTube, 'Micro blogging' applications, online gaming environments, and comment streams on public websites such as newspaper site etc. The growth of social media has been boosted by the fact that there is no longer a need to access it through a personal computer. Digital devices such as smartphones, tablets, laptops etc. easily connect users to the internet.

Cyber bullying is defined as any use of social media or communication technology to bully an individual or group e.g. taunts on line, by texts using social media platforms.

Many of the principles of this policy also apply to other types of online presence such as virtual worlds. The absence of, or lack of, explicit reference to a specific website or service does not limit the extent of the application of these guidelines. The internet and social media is driven by fast-paced evolving technology. Accordingly, it is not possible for the policy to cover every eventuality, but the principles set out in this policy must be followed irrespective of the medium.

Within this policy there is a distinction between the uses of the Partnerships sanctioned social media and personal use of social media.

5. Personal use of social media

- Staff employed by the Partnership are entitled to use whatever system they like outside their working time and working persona, to engage in the social aspects of the media. However, great care should be taken to ensure the private/work line is not crossed. It is good practice not to mention work, your opinions of your colleagues or processes and projects on your own private social media networks.

- Staff need to be aware of their online reputation and have to recognise that comments that they make online can be seen by others, particularly when using social networking sites. Staff should regard private social media with privacy settings as potentially public (i.e. viewed and shared to third parties) and anything they publish, whether they identify themselves as employees of the Partnership or not) may bring the Partnership into disrepute or call into question their suitability to work for the Partnership which could result in dismissal.
- There is an acknowledgment that the Partnership staff may/will have pre-existing engaged communications with parents from the community we serve. However, the Partnership staff are advised not to invite, accept or engage in communications with new parents and should not accept or engage in communications with children from the Partnership community in any personal social media whilst in the employment of the Partnership**.** Those pre-existing communications should be responsible and comply with the points listed below.
- Any communication received from children on any personal social media site must be reported to the ESL who will be responsible for referring this onto the designated safeguarding lead.
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Partnership staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts. All email communication between staff and members of the Partnerships community on work related business must be made from an official email account.
- Staff should not use personal email accounts or mobile phones to make contact with members of the Partnerships community on work related business, nor should any such contact be accepted, except in circumstances given prior approval by the Executive Headteacher.
- Staff are not permitted to refer to specific individual matters related to the Partnership and members of its community on any social media accounts.
- Staff are also advised to consider any reputation issues to the Partnership in any posts or comments related to the Partnership on any social media platforms.
- Staff should not accept any current pupil of any age or any ex-pupil of the Partnership under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.
- Where it is found that staff engage in the unacceptable use of social media in their private time using their personal social media accounts, it can be treated as misconduct (including gross misconduct) under the Partnership's policies.

6. School sanctioned use of social media

When using social media for educational/promotional purposes, the following practices should be observed.

- The content of any school-sanctioned social media site should be solely professional and should reflect well on the Partnership. Staff should use their work account, rather than their private social media account, to respond to comments/mentions on a Partnership sanctioned social media platform e.g. Twitter, Facebook etc.

- Staff must not publish photographs of children without the written consent of parents/ carers, identify by name any children featured in photographs, or allow person-identifying information to be published on school social media accounts
- Care must be taken that any links to external sites from the account are appropriate and safe
- Any inappropriate comments on, or abuse of, Partnership-sanctioned social media should immediately be reported to a member of the Senior Leadership Team (SLT) or the nominated E-safety lead. Where possible, care should be taken to preserve evidence of inappropriate comments/abuse (e.g. text, email, voicemail, website, instant message etc.) by taking screen prints of messages, web pages, images etc. in order that it can be investigated and relevant action taken
- The E- safety lead in conjunction with the Executive Headteacher will be responsible for determining the Partnership's responses to Partnership sanctioned social media platforms. This responsibility may be delegated to other staff from time to time.

7. Mobile technologies

- The Partnership allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the publicly accessible spaces. These are normally not to be used whilst children are present.
- Under no circumstances should staff use their own personal devices to contact children or parents either in or out of work time.
- Staff are not permitted to take photos or videos of children, using their own mobile devices. If photos or videos are being taken as part of the curriculum or for professional purposes, the Partnerships equipment will be used for this. Only Partnership phones should be used on trips for the purposes of recording pictures/videos etc.
- The Partnership is not responsible for the loss, damage or theft of any personal mobile device.

8. Communications

When using communication technologies, staff should consider the following as good practice:

- The official email service may be regarded as safe and secure and is monitored. Staff should be aware that email communications are monitored. Staff should use the Partnerships email services to communicate all business matters.
- Staff will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Staff must immediately report to their line manager/ESL/Executive Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature.
- Any digital communication between staff and the Partnership community must be professional in tone and content. These communications may only take place on official (monitored) systems.

- Personal information should not be posted on our website and only official email addresses should be used to identify members of staff. Staff should also refer to the list of Cybersafe –Do's and Don'ts in Appendix 1 of this policy.

9. Support for staff

Where staff have been the target of inappropriate, offensive, threatening, bullying/cyberbullying communication through digital means (whether in their professional or private life) which impacts on their ability to carry out their role effectively, they should expect the Partnership to:

- record such incidents – see Appendix 4
- investigate such incidents on behalf of staff
- respond to such incidents in a timely and appropriate manner, or support the member of staff concerned to do so
- provide appropriate support, or information enabling them to access appropriate personal support e.g. employee assistance scheme or occupational health
- support the member of staff to contact the police, external agencies or service provider where appropriate

10. Acceptable use of the Partnerships digital property

- Staff are responsible for any digital property belonging to the organisation that is under their control or in their possession and must take proper care of any such items
- Staff must take good care of our digital property, both when it is used in the workplace and when it is used outside the organisation's premises (e.g. at home)
- Staff must not make modifications to the digital property (for example, upgrades to a laptop or desktop) without the prior approval in writing of the Partnership.
- Staff must not use our digital property to carry out any illegal activities or activities that might bring the organisation into disrepute (for example, using a laptop to visit inappropriate websites).
- Staff must not, by act or omission, allow our digital property to be lost or damaged (for example, by not securing property properly or leaving it in a public place such as on public transport)
- Staff must immediately report any damage or faults involving equipment or software, however this may have happened.
- Staff must not remove any of our digital property from the premises without the prior approval of the Executive Headteacher or Chair of Governors
- On termination of their employment, staff will be required to return the Partnership's digital property on the date specified by the Executive Headteacher, which will normally be their last day at work. It is the member of staff's responsibility to return all of the organisations digital property
- The Partnership reserves the right to withhold the whole or any part of a member of staff's wages up to the market value of the digital property if he/she does not return that property by the set date. The amount withheld will be based on the estimated value of the property at that time

- In appropriate cases, the Partnership may contact the police about the unreturned property and/or issue civil proceedings against the member of staff for breach of contract and/or trespass to goods to the extent that any outstanding wages withheld do not cover the current market value of the property not returned

11. Monitoring of this policy

Any violation of this policy may be considered as potentially gross misconduct under the Partnership's Disciplinary Policy and Procedure (staff); Code of Conduct (staff); and under the Code of Practice (governors); which may result in disciplinary action being taken up to and including dismissal.

All staff and Governors are encouraged to report any suspicions of misuse to the Executive Headteacher/ESL. If the Executive Headteacher receives a disclosure that staff or a governor is using digital devices / social networking in an inappropriate way as detailed above, this should be dealt with in accordance with the Child Protection Policy and/or Disciplinary Policy and Procedure.

The Partnership has a duty of care to investigate and work with children and families where there are reports of cyber-bullying/misuse of social media during out of work hours.

12. The law

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, may be still subject to copyright, The General Data Protection Regulation, The Data Protection Act 2018 and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with government guidance on safeguarding children and the Partnership's Equalities and Child Protection policies.

Whilst there is no one specific offence of cyber-bullying, certain activities can be criminal offences under a range of different laws, including:

- The Protection from Harassment act 1997
- The Malicious Communications act 1988
- S.127 of the Communication act 2003
- Public Order Act 1986
- The Defamation Acts of 1952, 1996 and 2013

A school cannot be 'defamed'; only individuals or groups of individuals can bring action for defamation. Staff who are concerned that comments posted about them are defamatory in nature, should seek advice from their line manager/Executive Headteacher.

The Executive Headteacher may seek legal advice on any matters related to the potential misuse of social media.

Appendix 1

How to Stay 'Cybersafe' – Do's and Don'ts for the Partnership Staff

DO	DON'T
• be aware of your on-line reputation, which consists of information you post about yourself and information posted by others, and consider that when seeking employment, many prospective employers will use publicly available on-line information. Type your name into various search engines to see what information there is about you on the internet. Remember, the internet never forgets! • keep passwords secret and protect access to accounts – always lock or log off from any device that you have been using, even if you are only stepping out of the room for a moment and ensure that all phones and tablet devices are secured with a passcode; • regularly review your privacy settings on social media sites and your devices (mobile phone, tablet, laptop etc.); • discuss expectations with friends – are you happy to be tagged in photos? • be aware that, increasingly, individuals are being held to account in the courts for the things they say on social networking sites; • keep personal phone numbers private and don't use your own mobile phones to contact pupils or parents; • use the Partnerships mobile phone when on a trip; • keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on work premises and report thefts to the police and mobile operator as soon as possible (Note: you can find out your IMEI number by typing *#06# on your handset – the number will be displayed on the screen); • ensure that rules regarding the use of technologies are consistently enforced; • report any incident to the appropriate member of staff in a timely manner; • keep any evidence of an incident, for	• post information and photos about yourself, or work-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see; • befriend pupils or other members of the Partnership community on social networking sites. (You should consider carefully the implications of befriending parents or ex-pupils). • personally retaliate to any incident, bullying messages; • criticise your nursery school, children's centre, children or children's parents online.

example by not deleting text messages or e-mails and by taking a screen capture of material (staff need to be aware that taking a screenshot of content which is potentially illegal could result in staff committing a criminal offence) including the URL or web address. • maintain an online safety incident report log (Appendix 4) • use Partnership e-mail address only for work purposes. • be aware that if you access any personal web-based e-mail accounts via the Partnerships network, that these may be subject to our internet protocol which could include monitoring and surveillance. • request assurances from management that any e-mails marked 'personal' and/or 'union business' will not be read without your prior consent. • raise genuine concerns about the Partnership or certain members of staff using your employer's whistle blowing or grievance procedure.	

More helpful tips are available from the UK Safer Internet Centre at www.saferinternet.org.uk under 'Advice and Resources'.

Appendix 2

Contact details for the Partnership's E-Safety Lead

Name	**[insert relevant name]**
School & Children's Centre address	**[insert relevant address]**
Contact number	**[insert relevant school contact number]**

Appendix 3

Staff Declaration

I have read and understand the E-Safety Policy (Brent Adopted Digital Safety/ Social Media Policy and Acceptable Use) and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal.

I understand that, in certain circumstances, inappropriate use of Social Media may become a matter for police or social care investigations.

I understand that if I need any clarification regarding my use of Social Media, I can seek such clarification from any member of the Senior Leadership Team.

I confirm that I understand the E-Safety Policy (Brent Adopted Digital Safety/ Social Media Policy and Acceptable Use) and have been given the opportunity to raise any queries or questions about the policy and have these satisfactorily addressed before signing this declaration.

SIGNED:
…….

NAME: …….

DATE:
…….

Appendix 4: Online Safety Incident Report Log

Online safety incident report log				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**