Digital/Online Safety and Acceptable Use Policy for Schools

March 2021

Adopted by the Governing Board of Roe Green Junior School.

Chair V. Assani Date September 2025

Review date September 2026

Contents Page

1. Introduction

Computing and the use of digital 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, 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.

Computing and 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 school governing body, all teaching/support and other staff, whether employed directly by the school or through a hiring organisation (e.g. agency), external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. 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 school's reputation, school 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 School into disrepute.
- safeguard all children and staff.
- ensure that where information is provided through social media regarding the School, this is representative of the school.

3. Roles and responsibilities

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

The Headteacher will ensure that the School has a nominated Digital Safety Lead tasked with overseeing and managing the recording, investigation and resolution of digital safety incidents. Contact details for the School's Digital Safety Lead is attached as an appendix to this policy. The nominated Digital Safety Lead will be suitably trained in order to undertake this role. The 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 4 to confirm they have read and understood the Digital Safety/Social Media and Acceptable Use Policy.

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 but are not limited to 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 a 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 school-sanctioned social media and personal use of social media.

5. Personal use of social media

5.1 Staff employed by the School 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 or public social media networks. There is also a recognition that staff/school leaders may use their social media accounts for professional use to share best practice; however where this occurs confidentiality issues must be strictly observed. Where the school's behaviour policy/code of conduct explicitly prevents mentioning work/opinions of colleagues/processes/projects within private or public social media networks, this should be observed.

5.2 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). Regardless of whether the employee has identified themselves as school employees or not, anything they publish either school related, or another matter which may bring the School into disrepute, or call into question their suitability to work at the School, could result in dismissal. Employees should ensure they monitor the responses of comments made on their own social media accounts and remove them if damaging to the school or its employees where this is brought to their attention.

5.3 There is an acknowledgment that school staff may/will have pre-existing engaged communications with parents from the school community. However, school 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 school community in any personal social media whilst in employment at the School**.** Those

pre-existing communications should be responsible and comply with the points listed below.

5.4 Any communication received from children on any personal social media site must be reported to the Digital Safety Lead who will be responsible for referring this onto the Designated Safeguarding Lead.

5.5 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.

5.6 School staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.

5.7 All email communication between staff and members of the school community on school business must be made from an official school email account.

5.8 Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headteacher.

5.9 Staff are not permitted to refer to specific individual matters related to the School and members of its community on any social media accounts.

5.10 Staff are also advised to consider any reputation issues to the School in any posts or comments related to the School on any social media platforms. Where the school has a behaviour policy/code of conduct preventing the posting of comments on social media platforms related to the school, this should be observed.

5.11 Special consideration may be given on the above three points if it is for the purpose of trade union activity; which should be conducted within private member-only groups and in line with the union's own GDPR policies, and should not be shared or copied outside these private memberships. Staff are still expected to observe the school's/trade union's codes of conduct in such communications and where appropriate utilise the school's procedures to address any concerns they may have with the school or its staff.

5.12 Staff should not accept any current pupil of any age or any ex-pupil of the School under the age of 18 as a friend, follower, subscriber or similar on any personal social media account.

5.13 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 School's policies.

6. School-sanctioned use of social media

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

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

6.2 Staff must not publish photographs of children or staff without the written consent of parents/ carers/ staff, identify by name any children or staff featured in photographs, or allow person-identifying information to be published on school social media accounts. Schools may wish to use their established GDPR consent mechanisms to ensure the school complies with this requirement. Schools should ensure periodic review of such mechanisms to ensure they are robust in this regard.

6.3 Care must be taken that any links to external sites from the account are appropriate and safe.
6.4 Any inappropriate comments on, or abuse of, school-sanctioned social media should immediately be reported to a member of the Senior Leadership Team (SLT) or the nominated Digital 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.
6.5 The Digital Safety Lead in conjunction with the Headteacher will be responsible for determining the School's responses to school sanctioned social media platforms. This responsibility may be delegated to other staff from time to time.

7. Mobile technologies

7.1 The School allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are normally not to be used whilst children are present.
7.2 Staff should not use their own personal devices to contact pupils or parents either in or out of school time. Any exception to this must be authorised by school leaders and appropriate measures put in place.
7.3 Staff are not permitted to take photos or videos of pupils on their personal mobile phones. If photos or videos are being taken as part of the school curriculum or for professional purposes, the school equipment will be used for this. Only school phones should be used on school trips for the purposes of recording pictures/videos etc. and for emergency contact purposes.
7.4 The School is not responsible for the loss, damage or theft of any personal mobile device.

8. School sanctioned remote learning platforms

8.1 Staff will only use school sanctioned platforms which have been assessed and approved by the Senior Leadership Team for remote learning in the school.
8.2 The school has adopted the Template Acceptable Use Policy (AUP) for Remote Learning and Online Communication (see appendix 4).

9. Communications

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

9.1 The official school 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 school email services to communicate school business. The exception is that personal emails and trade union email accounts can be used in addition for trade union communications as long as it is used in line with the unions' own GDPR policies and the school's/union's codes of conduct.
9.2 Staff must immediately report to their line manager, Digital Safety Lead or Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature.
9.3 Any digital communication between staff and the school community must be professional in tone and content. These communications may only take place on official (monitored) school systems.
9.4 Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9.5 Photos of staff should not be posted on the school website unless staff have given consent for this. Schools may wish to use their established GDPR consent mechanisms to ensure the school complies with this requirement. Schools should ensure periodic review of such mechanisms to ensure they are robust in this regard.

Staff should also refer to the list of Cybersafe –Do's and Don'ts in Appendix 1 of this policy.

10. 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 their ability to carry out their role effectively, they should expect the School to:

10.1 Record such incidents in writing.
10.2 Investigate such incidents on behalf of staff.
10.3 Respond to such incidents in a timely and appropriate manner, or support the member of staff concerned to do so.
10.4 Provide appropriate support, or information enabling them to access appropriate personal support e.g. employee assistance scheme or occupational health.
10.5 Support the member of staff to contact the police, external agencies or service provider where appropriate (see Appendix 2 for contact details for service providers).
10.6 Take appropriate action against the perpetrator in line with the relevant school policies where this falls within the schools jurisdiction.

11. Acceptable use of school digital property

11.1 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.
11.2 Staff must take good care of school digital property, both when it is used in the workplace and when it is used outside the organisation's premises (e.g. at home).
11.3 Staff must not make modifications to the school's digital property (for example, upgrades to a laptop) without the prior approval in writing of the School.
11.4 Staff must not use school 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).
11.5 Staff must not, by act or omission, allow school 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) however the school should ensure they are insured where possible for such eventualities if staff are required to participate in remote and/or working from home.
11.6 Staff must not remove any school digital property from the school's premises without the prior approval of the Headteacher or Chair of Governors.
11.7 On termination of their employment, staff will be required to return the school's digital property on the date specified by the Headteacher, which will normally be their last day at work. It is the member of staff's responsibility to return school digital property.

11.8 The School reserves the right to withhold the whole or any part of a member of staff's wages up to the market value of the school's 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.

11.9 In appropriate cases, the school 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.

12. Monitoring of this policy

Any violation of this policy may be considered as potentially gross misconduct under the school'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 Headteacher/Digital Safety Lead. If the 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 school 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 school hours.

13. 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 school'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/Headteacher.

The Headteacher may seek HR/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 school 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 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 a school mobile phone when on a school trip; • keep a record of your phone's unique International Mobile Equipment Identity (IMEI) number, keep phones secure while on school 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);	• post information and photos about yourself, or school-related matters, publicly that you wouldn't want employers, colleagues, pupils or parents to see; • befriend pupils or other members of the school 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 school, pupils or pupils' parents online.

• ensure that school 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 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. • use school e-mail address only for work purposes. • be aware that if you access any personal web-based e-mail accounts via the school network, that these may be subject to the school's 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 your school 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'.

The NEU have developed further guidance on livestreaming sessions which can be observed at the following link: https://neu.org.uk/coronavirus-livestreaming-lessons

Appendix 2

Contact details for service providers

Service provider	From your mobile	Pay as you go	Pay monthly contracts
O2	202 (pay monthly) 4445 (pay as you go)	03448 090 222	03448 090 020
Vodaphone:	191	08700 776 655	08700 700 191
3	333	08707 330 333	08707 330 333
EE (Orange and T Mobile)	150	07953 966 250	07953 966 250
Virgin	789	0345 6000 789	0345 6000 789
BT		08000 328 751	08000 328 751

Appendix 3

Contact details for the School's Digital Safety Lead

Name	Melissa Loosemore Dan Guest Romina da Silva
School address	Roe Green Junior School, Princes Avenue Kingsbury, NW9 9JL
Contact number	020 8204 5221 Ex 2

Appendix 4

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- That school ICT systems and users are protected from accidental or deliberate misuse.

Name of Staff Member/Governor/Volunteer/Visitor:……

When using my own device or the school's ICT facilities including remote access and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
- Use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Head teacher.
- Use them in any way which could harm the school's reputation.
- Use any improper language when communicating online, including in emails or other messaging services.
- Install any unauthorised software or connect unauthorised hardware or devices to the school's network.
- Share my password with others or log in to the school's network using someone else's details.
- Share confidential information about the school, its pupils or staff, or other members of the community.
- Access, modify or share data I'm not authorised to access, modify or share.
- Promote private businesses, unless that business is directly related to the school.

I will:

- Adhere to all requirements of the schools Data Protection Policy in accordance to GDPR.

- Ensure all email communication between myself and members of the school community on school business will be made from my official school email account

- Only use encrypted Storage devices such as USBs /Hard drives for sensitive data in line with GDPR regulations.

- Understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

- Take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

- Let the designated safeguarding lead (DSL) and Network manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

- Only use LGFL's Microsoft Staff Mailing system for school related business.

- Always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (Staff Member/Governor/Volunteer/Visitor):…….

Date:…….

Signed (Head Teacher/Deputy Head/Assistant Head):…….

Name Printed (Head Teacher/Deputy Head/Assistant Head):…….

Date:…….

Staff Declaration

I have read and understand the Digital/Online Safety and Acceptable Use Policy for Schools 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 Digital Safety/ Social Media Policy and Acceptable Use of Property Policy 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: ……..

PRINT NAME: ……

DATE: ……..