Nexus Education Schools Trust

Online-Safety Policy

Farnborough Primary School

Date: September 2018

Review Date: September 2020

Online-Safety Policy

Contents

Key People....3

1. Overview 4

2. Further Help and Support....4

3. Scope 4

4. Roles & Responsibilities....4

4.1 Headteacher – Angela James 5

4.2 Designated Safeguarding Lead (DSL) – Angela James....5

4.3 Local Committee 6

4.4 All Staff 7

4.5 Computing Curriculum Lead – Caroline Roberts....8

4.6 Subject Leads 8

4.7 Network Manager/IT Technician – ADEPT/Shirley Pugh....8

4.8 Data Protection Officer – Chorus Advisors 9

4.9 LGfL TRUSTnet Nominated Contacts – ADEPT/Shirley Pugh 9

4.10 Volunteers and Contractors....9

4.11 Pupils 10

4.12 Parents/Carers....10

4.13 External Groups including Parent Associations – FPS PTA & Farnborough Kids Club ..10

5. Education and Curriculum 10

6. Handling Online-Safety Concerns and Incidents....11

7. Actions where there are concerns about a child 13

8. Sexting....14

9. Bullying 15

10. Sexual Violence and Harrassment....15

11. Misuse of School Technology (devices, systems, networks or platforms) 15

12. Social Media Incidents 15

13. Data Protection and Data Security....15

14. Appropriate Filtering and Monitoring....16

15. Electronic Communications 17

16. Email 17

17. School Website 17

18. Cloud Platforms 18

19. Digital Images and Video....18

20. Social Media....19

21. Staff, Pupils and Parents’ Social Media Presence 20
22. Device Usage 21
22.1 Personal Devices used in School Policy 21
22.2 Trips/events away from School 21
22.3 Searching and Confiscation 21
23. References/Appendices 21

Key People

Designated Safeguarding Lead (DSL) : Angela James- Headteacher

Safeguarding Local Committee Member : Susan Donovan

Data Protection Officer (DPO):
Chorus Advisers - dpo@chorusadvisers.co.uk

1. Overview

This policy aims to:

- Set out expectations for all Farnborough Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Child Protection & Safeguarding Policy, Behaviour Policy or Anti-Bullying Policy)

2. Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

3. Scope

This policy applies to all members of the Farnborough Primary school community (including staff, local committee members, volunteers, contractors, pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

4. Roles & Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

4.1 Headteacher – Angela James

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the Designated Safeguarding Lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance (Keeping Children Safe in Education, Sept 2018) and relevant Local Safeguarding Children Board (LSCB) guidance.
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and Local Committee to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure Local Committee members are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory DfE requirements (see appendices for website audit document).

4.2 Designated Safeguarding Lead (DSL) – Angela James

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2018):

- "The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Ensure "An effective approach to online safety [that] empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children".

- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Headteacher, Trust and Local Committee members to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safety – the new LGfL DigiSafe **pupil survey** of 40,000 pupils may be useful reading (new themes include 'self-harm bullying' and getting undressed on camera).
- Review and update this policy in line with NEST, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for Behaviour, Child Protection & Safeguarding, Prevent and others) and keep the Local Committee informed.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCCIS framework 'Education for a Connected World') and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT to discuss current issues (anonymised).
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Use LGfL filtering systems and ensure staff are aware these are in place.
- Ensure the 2018 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - **cpd.lgfl.net** has helpful CPD materials including PowerPoints, videos and more

4.3 Local Committee

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2018):

- "Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the DLS and incorporate online safety into standing discussions of safeguarding at Local Committee meetings.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.

- Work with the Trust, DSL and Headteacher to ensure a GDPR-compliant framework for storing data but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction and regularly updated [annually] in line with advice from the LSCB online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at **cpd.lgfl.net**
- "Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". LGfL's appropriate filtering submission is **here**
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety with a clear policy on the use of mobile technology."

4.4 All Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead (DSL) is; **Angela James**.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main Child Protection & Safeguarding policy.
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff Acceptable Use Policy and Code of Conduct/Handbook.
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem.

- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know.
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey of 40,000 pupils (new themes include 'self-harm bullying' and getting undressed on camera).
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.

4.5 Computing Curriculum Lead – Caroline Roberts

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the National Curriculum.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

4.6 Subject Leads

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike.
- Consider how the UKCCIS framework Education for a Connected World can be applied in your context.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.

4.7 Network Manager/IT Technician – ADEPT/Shirley Pugh

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the DSL/Trust/LGfL TRUSTnet nominated contact to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and Senior Leadership Team.

- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Network managers/technicians at LGfL TRUSTnet schools may want to ensure that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish (from Sept 2018), Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress (from Sept 2018), Meraki Mobile Device Management and CloudReady/NeverWare. These solutions which are part of your package will help protect the network and users on it.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy.

4.8 Data Protection Officer – Chorus Advisers

Key responsibilities:

- NB – this document is not for general data-protection guidance; GDPR information on the relationship between the school and LGfL TRUSTnet can be found at gdpr.lgfl.net; there is an LGfL document on the general role and responsibilities of a DPO in the 'Resources for Schools' section of that page. Full GDPR information for the Trust can be found at www.nestschools.org
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (April 2018), especially this quote from the latter document:
    - GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place […] Remember, the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding.
- The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'.
- Work with the GDPR Lead at NEST who will liaise with the Headteacher to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

4.9 LGfL TRUSTnet Nominated Contacts – ADEPT/Shirley Pugh

Key responsibilities:

- To ensure all LGfL TRUSTnet services are managed on behalf of the school in line with school policies, following data handling procedures as relevant.

4.10 Volunteers and Contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP).

- Report any concerns, no matter how small, to the Designated Safeguarding Lead as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

4.11 Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's Acceptable Use Policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

4.12 Parents/Carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

4.13 External Groups including Parent Associations – Farnborough PTA/Farnborough Kids Club (and any other external after school clubs which may wish to use school technology or the internet within the school)

Key responsibilities:

- Any external individual/organisation will sign an Acceptable Use Policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, local committee members, contractors, pupils or other parents/carers.

5. Education and Curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Health Education, Relationships (in secondaries: Relationships and Sex) Education (being implemented from September 2019 for September 2020)

- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Farnborough Primary School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCCIS (the UK Council for Child Internet Safety, soon to become UKCIS, no longer solely for children). The computing curriculum includes at least one half term fully dedicated to E-Safety for each year group and we always include some E-Safety aspect to any lesson where children are using technology, across all subjects. We cover most of the things that are mentioned on the framework already and continue to review as necessary.

6. Handling Online-Safety Concerns and Incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE, Citizenship and (from September 2019 for September 2020) the new statutory Health Education and Relationships Education.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with child protection with regards to online-safety will be handled in line with the following policies:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

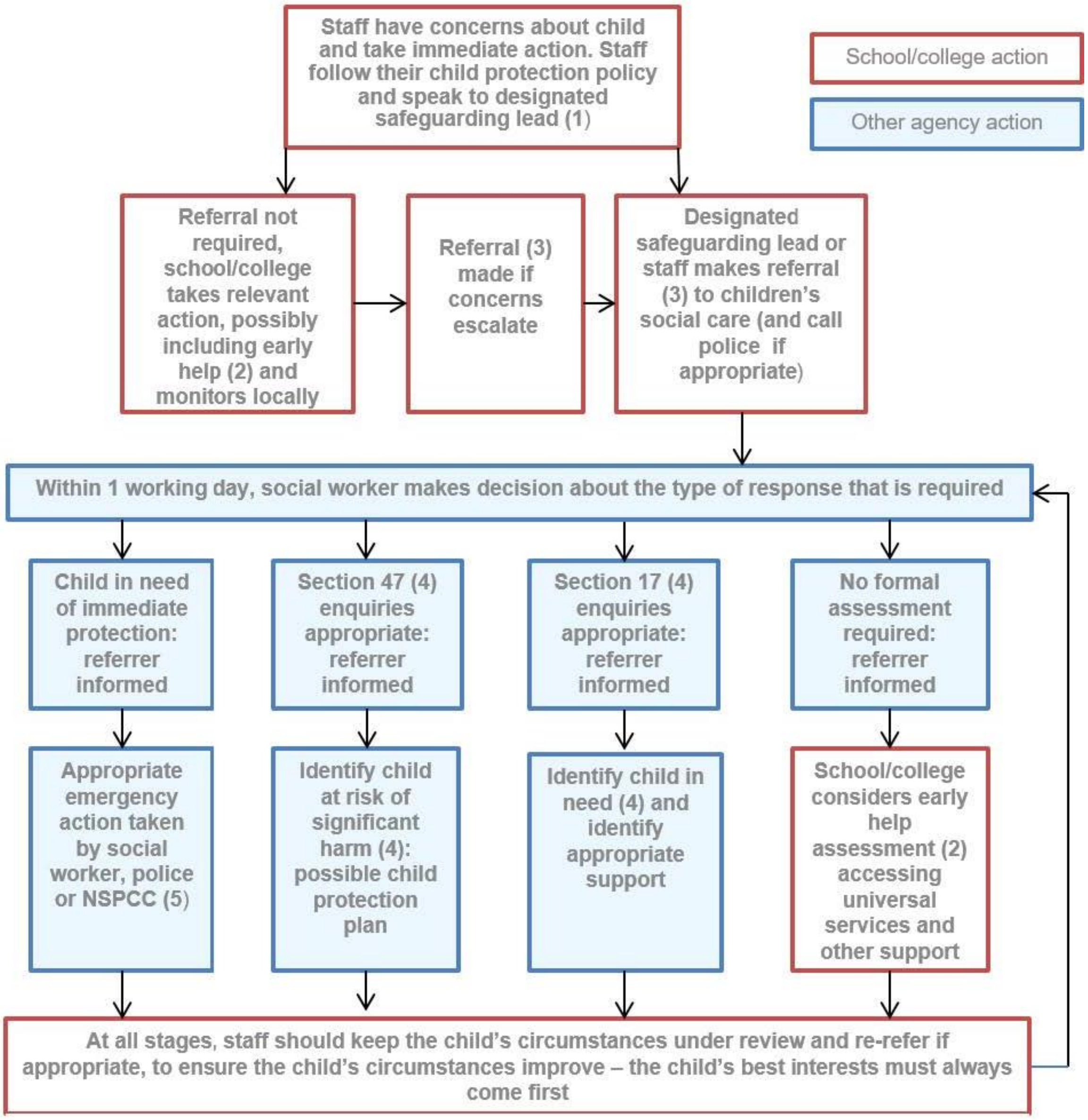
Any suspected online risk or infringement should be reported to the online safety lead / DSL on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Local Committee and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room – see posters.lgfl.net and reporting.lgfl.net).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (procedures are in place for sexting; see section below).

7. Actions where there are concerns about a child

The following flowchart is taken from page 13 of Keeping Children Safe in Education 2018 as the key education safeguarding document.



School/college action

Other agency action

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead (1)

Referral not required, school/college takes relevant action, possibly including early help (2) and monitors locally

Referral (3) made if concerns escalate

Designated safeguarding lead or staff makes referral (3) to children's social care (and call police if appropriate)

Within 1 working day, social worker makes decision about the type of response that is required

Child in need of immediate protection: referrer informed

Section 47 (4) enquiries appropriate: referrer informed

Section 17 (4) enquiries appropriate: referrer informed

No formal assessment required: referrer informed

Appropriate emergency action taken by social worker, police or NSPCC (5)

Identify child at risk of significant harm (4): possible child protection plan

Identify child in need (4) and identify appropriate support

School/college considers early help assessment (2) accessing universal services and other support

At all stages, staff should keep the child's circumstances under review and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

(1) In cases which also involve an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of Working together to safeguard children provides detailed guidance on the early help process.

(3) Referrals should follow the local authority's referral process. Chapter one of Working together to safeguard children.

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. This can include section 17 assessments of children in need and section 47 assessments of children at risk of significant harm. Full details are in Chapter One of Working together to safeguard children.

(5) This could include applying for an Emergency Protection Order (EPO).

8. Sexting

All schools (regardless of phase) should refer to the UK Council for Child Internet Safety (UKCCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools.

There is a one-page overview for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

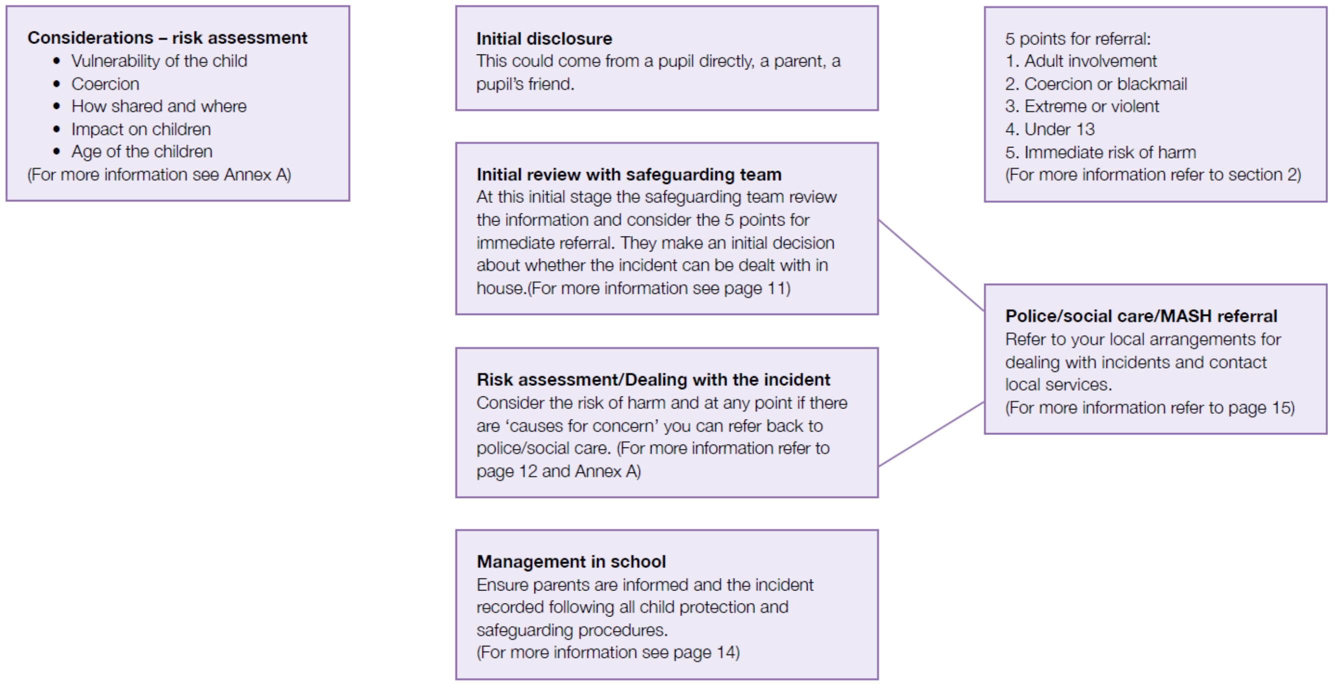
The school DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Annex G

Flowchart for responding to incidents



Considerations – risk assessment
- Vulnerability of the child
- Coercion
- How shared and where
- Impact on children
- Age of the children

(For more information see Annex A)

Initial disclosure
This could come from a pupil directly, a parent, a pupil's friend.

Initial review with safeguarding team
At this initial stage the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house.(For more information see page 11)

Risk assessment/Dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer back to police/social care. (For more information refer to page 12 and Annex A)

Management in school
Ensure parents are informed and the incident recorded following all child protection and safeguarding procedures.
(For more information see page 14)

5 points for referral:
1. Adult involvement
2. Coercion or blackmail
3. Extreme or violent
4. Under 13
5. Immediate risk of harm

(For more information refer to section 2)

Police/social care/MASH referral
Refer to your local arrangements for dealing with incidents and contact local services.
(For more information refer to page 15)

9. Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. It is important not to treat online bullying separately to offline bullying and to recognise that much bullying will often have both online and offline elements.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

10. Sexual Violence and Harrassment

In 2018 new Department for Education guidance was issued on sexual violence and harassment, as a new section within Keeping Children Safe in Education and as a document in its own right.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate.

11. Misuse of School Technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document.

Where pupils contravene these rules, the school Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff Code of Conduct/Handbook.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology.

12. Social Media Incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Farnborough Primary community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school Behaviour Policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Farnborough Primary School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

13. Data Protection and Data Security

This section serves to highlight general principles regarding the relationship between safeguarding and data protection / data security, and to signpost to useful information.

GDPR information on the relationship between the school and LGfL TRUSTnet can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

“GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent.

When DSLs in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and or parent/carer that should also be recorded within the safeguarding file.

All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, **appropriate organisational and technical safeguards should still be in place.** Remember, **the law does not prevent information about children being shared with specific authorities if it is for the purposes of safeguarding**.”

All pupils, staff, local committee, volunteers, contractors and parents are bound by NEST’s Data Protection Policy and agreements, which can be found here on our school website.

Rigorous controls on the LGfL TRUSTnet network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL TRUSTnet services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The Headteacher, Trust and local committee work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Staff must ensure that only encrypted USB sticks are used when working on documents away from school. The school should provide these encrypted USB sticks and keep a log of who has these.

14. Appropriate Filtering and Monitoring

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

At this school, the internet connection is provided by LGfL TRUSTnet. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre’s appropriate filtering submission pages here.

15. Electronic Communications

This section only covers electronic communications, but the principles of transparency, appropriate conduct and audit trail apply.

16. Email

- Pupils at this school do not currently have individual email accounts. We are hoping in the future that KS2 pupils will have an LGFL USO login which will be restricted for use in the school only.
- Staff at this school use the StaffMail for all school emails

Staffmail linked to the USO authentication system and are fully auditable, trackable and managed by LGfL TRUSTnet on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the DPO / Headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL TRUSTnet. Data (except child protection information) can be sent using the email system but the document must be password protected and the password sent separately from the file once the recipient has confirmed receipt.
    - Internally, staff should use the school network
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- Pupils are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

17. School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Local Committee have delegated the day-to-day responsibility of updating the content of the website to Mrs G Ellson. The site is managed by / hosted by Frootes Media.

The Department for Education has determined information which must be available on a school website. LGfL TRUSTnet has compiled RAG (red-amber-green) audits to help schools to ensure that are requirements are met (see appendices).

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL TRUSTnet schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected, and full names are not published (remember also not to save images with a filename that includes a pupil's full name). Staff must check that permission has been given before publishing photos of children.

18. Cloud Platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the Department for Education document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our Data Protection policy.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The following principles apply:

- Any new cloud systems should be subject to a DPIA (data-protection impact statement) and parental permission will need to be sought.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by pupil or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

19. Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos and for what purpose (beyond internal assessment, which does not require express consent). Parents answer as follows:

- For displays around the school
- For assessment purposes
- For marketing/media purposes (School website, newsletter, prospectus)
- Videos for assessment purposes, Christmas productions

- Photos/videos for use by NEST (website, newsletters, prospectus)

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At Farnborough Primary School no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

20. Social Media

Farnborough Primary School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner, even though there are no official/active school social media accounts.

21. Staff, Pupils and Parents' Social Media Presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use Policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school Complaints Procedure which can be found on our website, should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school, and between staff and pupils. Parents/Carers need to send all emails through the school office using admin.office@farnborough.bromley.sch.uk .

Pupils are not allowed to be 'friends' with or make a friend request to any staff, Local Committee members, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, Local Committee members, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 19) and permission is sought before uploading photographs, videos or any other information about other people.

22. Device Usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

22.1 Personal Devices used in School Policy

- **Pupils in Year 6** are allowed to bring mobile phones in for emergency use only and these must be handed to the Class Teacher at the start of the day. During lessons, phones must remain turned off at all times. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital Images and Video section on page 19, and Data Protection and data security section on page 16. Child/staff data should never be downloaded onto a private phone. **Volunteers, contractors, Local Committee members** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** Parents are asked to leave their phones in their pockets and turned off when they are on site in school buildings. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital Images and Video section on page 19. [parentfilming.lgfl.net may provide further useful guidance].

22.2 Trips/events away from School

For school trips/events away from school, teachers may use their personal phone for any authorised or emergency communications with pupils/staff and parents. The phone must not be used for taking any photographs or video. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number, by dialing '141' before the number. Wherever possible, the teacher will phone the School Office and ask them to make the call.

Parents accompanying school trips must be reminded not to use their mobile phones or take any photographs or videos of ANY children.

22.3 Searching and Confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

In most cases, the school will work with the pupil/parent concerned.

23. References/Appendices

1. Safeguarding Incident log (As detailed in Child Protection and Safeguarding Policy)
2. Child Protection and Safeguarding Policy
3. Behaviour Policy and Anti-Bullying Policy
4. Staff Code of Conduct/Handbook

5. Acceptable Use Policies for:
    - Staff, Volunteers, Local Committee & Contractors
    - Pupils (including SEND)
    - Parents
6. Consent form for taking and using photos & videos
7. Safer Working Practice for those working with children and young people in education (Safer Recruitment Consortium)
8. Working Together to Safeguard Children 2018 (DfE)
9. Keeping Children Safe in Education 2018 (DfE)
10. Searching, Screening and Confiscation Advice (DfE)
11. Sexual Violence and sexual harassment between children in schools and colleges (DfE)
12. Sexting Guidance from UKCCIS
13. Prevent Duty Guidance for Schools (DfE and Educate Against Hate)
14. Cyber Bullying: advice for Headteachers and School Staff (DfE)
15. RAG audits for statutory requirements of school websites
16. LGfL DigiSafe pupil survey
17. UKCCIS framework Education for a Connected World

Additional information and templates can be found at safepolicies.lgfl.net