Online Safety Policy

Responsibility	Pupils, Parents and Community	
Status	Recommended	
Ratification date	10.07.2018	
Review cycle / date	2 Year	Summer 2020
Reference	049.3	
Last updated	19.07.2019	

1 Introduction

1.1 Key people / dates

Designated Safeguarding Lead (DSL) team Deputy DSL Deputy DSL	Lee Cornwall Pippa Wright Kelly Dooley
Online-safety coordinator	Lee Cornwall
Safeguarding link governor Online safety link governor	Cathy Bird Rachael Prasher
Network manager	ClickOn IT London
Data, Systems and CS	Deesh Grewal
RTS website RTS Twitter account	Head Teacher's PA Head Teacher's PA, Chloe Speed
Date this policy was reviewed and by whom	05.10.2018 by Deesh Grewal
Date of next review and by whom	Autumn 2019 by Deesh Grewal

1.2 What is this policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with *Keeping Children Safe in Education 2018 (KCSIE)* and other statutory documents; it is designed to sit alongside our statutory Safeguarding Policy. Any issues and concerns with online safety must follow RTS's safeguarding and child protection procedures.

2.3 Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year, in response to developments in the school and local area.
Although many aspects will be informed by legislation and regulations, we involve staff, trustees, students and parents in writing and reviewing the policy (Section 78 of KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Changes to this policy will be disseminated to all the above stakeholders.

2.4 Who is in charge of online safety?

The DSL at RTS will take lead responsibility for online safety, in line with KCSIE

> "the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."

The DSL will monitor and review online safety with the Data, Systems and CS lead.

2.5 What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct Professor Tanya Byron: "Safer children in a digital world", 2008). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

The LGfL DigiSafe 2018 pupil survey of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

2.6 How will this policy be communicated?

This policy aims to impact upon practice and is therefore a living document. It is accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the Staff Notices classroom
- Available in paper format in the staffroom
- Part of the RTS induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, trustees, pupils and parents/carers (in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in all classrooms
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

3 Contents

4 Overview

4.1 Aims

This policy aims to:

- Set out expectations for all The Richmond upon Thames 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 Behaviour Policy or Anti-Bullying Policy)

4.2 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 Safeguarding Policy.

The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the Head Teacher will handle referrals to the LA designated officer (LADO).

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.

4.3 Scope

This policy applies to all members of the Richmond upon Thames School community (including staff, trustees, volunteers, contractors, students/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.

5 Roles and 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.

5.1 Head Teacher – Kelly Dooley

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 and relevant Local Safeguarding Children Board (LSCB) guidance
- Liaise with the designated safeguarding lead 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 trustees 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 IT 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 suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- 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 trustees 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)
- Report all online safety concerns as outlined in the RTS safeguarding policy (via ProvisionMap)

5.2 Designated Safeguarding Lead/ Online Safety Lead – Lee Cornwall

Key responsibilities

The DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility

The above 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 or college to protect and educate the whole school or college 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 Head Teacher, DPO and trustees 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, including signing up to the LGfL dsl mailing list. This regular communication provides access to the latest issues and also provides guidance on emerging issues eg *self-harm bullying* and *getting undressed on camera*

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the trustees/trustees.
- 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 and the designated online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring can be improved
- 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
- Oversee and discuss *appropriate filtering and monitoring* with trustees and ensure staff are aware
- 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

5.3 Trust Board, led by Online Safety / Safeguarding Link Trustees – Rachael Prasher /Cathy Bird

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

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCCIS) **Online safety in schools and colleges: Questions from the Governing Board**
- "Ensure an appropriate senior member of staff, from the school or college 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 online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor 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 DPO, DSL and Head Teacher 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 […] 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." NB – you may wish to investigate/adopt the UKCCIS cross-curricular framework 'Education for a Connected World' to support a whole-school approach

5.4 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) and Online Safety Lead (OSL) is **Lee Cornwall**
- 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 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
- Notify the DSL/OSL if the 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/stage/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 protection law
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- 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/OSL know
- Receive regular updates from the DSL/OSL 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.
- Report all online safety concerns as outlined in the RTS safeguarding policy (via ProvisionMap)

5.5 PSHCEE / PRE – Lee Cornwall

Key responsibilities from September 2019 for September 2020 (quotes taken from DfE press release on 19 July 2018 on *New relationships and health education in schools*):

As listed in the 'all staff' section, plus:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCEE / PRE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHCEE / PRE.

5.6 Computing Curriculum Lead – Deesh Grewal

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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

5.7 Curriculum and other leaders

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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Report all online safety concerns as outlined in the RTS safeguarding policy (via ProvisionMap)

5.8 Network Manager and technicians – ClickOn IT London

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 designated safeguarding lead / online safety lead / data protection officer / 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
- Take advantage of LGfL solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress and Meraki Mobile Device Management
- 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
- Work with the Head Teacher to ensure the school website meets statutory DfE requirements (see appendices for website audit document)
- Report all online safety concerns as outlined in the RTS safeguarding policy (via ProvisionMap)

5.9 Data Protection Officer (DPO) – David Coy (GROW education partners)

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

- Be aware 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 DSL, Head Teacher and trustees 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

5.10 LGfL TRUSTnet Nominated contact – Deesh Grewal

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
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services, including GSuite
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL TRUSTnet at gdpr.lgfl.net

5.11 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 safety lead / online safety coordinator 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

5.12 Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/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

5.13 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, trustees, contractors, pupils or other parents/carers.

The LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety but only half talk about it with them more than once a year

5.14 External groups including parent associations (FoRTS)

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, trustees, contractors, pupils or other parents/carers

6 Education and curriculum

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

- PSHCEE
- Health Education, 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/stage/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/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).

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 The Richmond upon Thames 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).

Annual reviews of curriculum plans (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of:

- Self-image and Identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership

7 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, PSHCEE, Citizenship* and (from September 2019 for September 2020) the new statutory *Health Education and Relationships* and *Sex 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 online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection (including Sexual Harassment / Peer on Peer Abuse) Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Policy
- Data Protection and GDPR 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 / designated safeguarding lead 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 Head Teacher, unless the concern is about the Head Teacher in which case the complaint is referred to the Chair of trustees and the LADO (Local Authority Designated Officer).

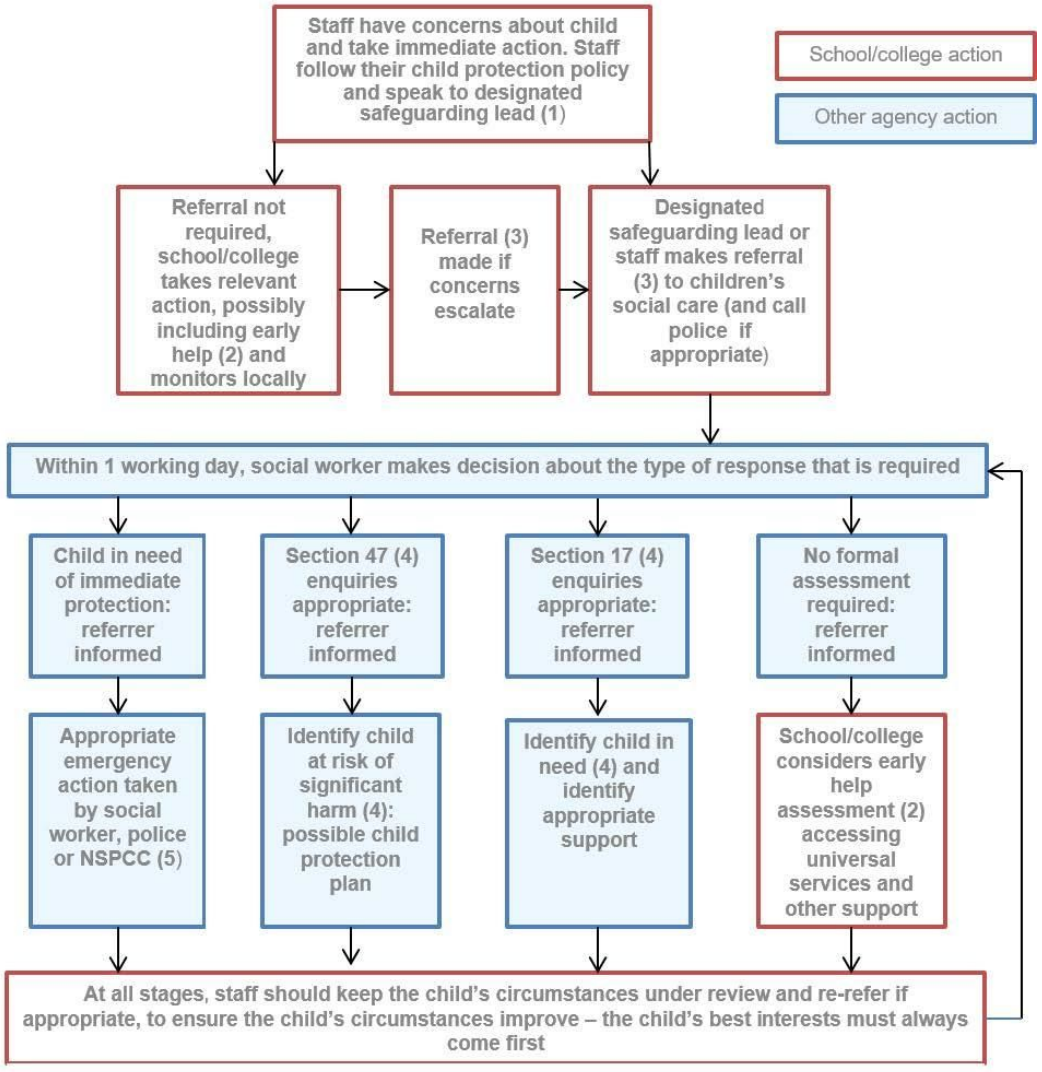
Staff may also use the NSPCC Whistleblowing Helpline (details of their helpline are displayed in the staff room – see posters.lgfl.net and reporting.lgfl.net).

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 (particular procedures are in place for sexting; see section below).

7.1 Actions where there are concerns about a child

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2018 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(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).

7.2 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. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

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.**

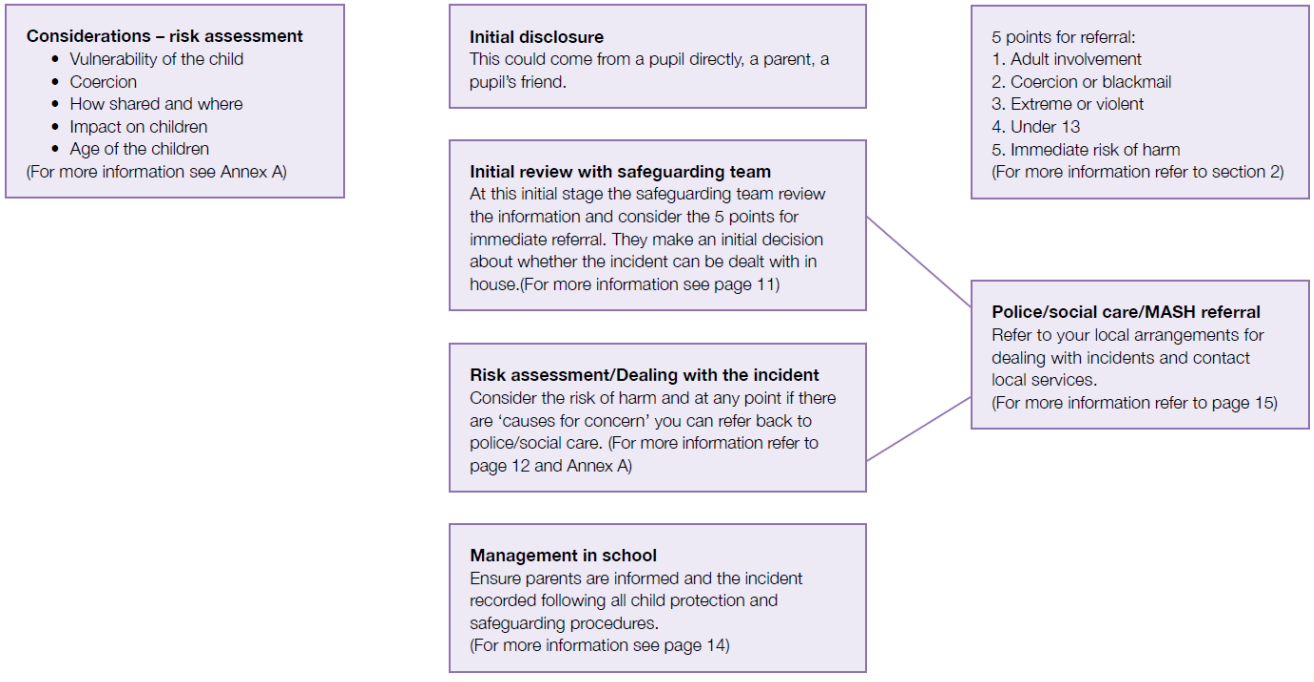
The DSL will in turn use the full 50-page guidance document including case studies, typologies and a flow chart as shown below (for information only, must be viewed in the context of the full document) to decide next steps and whether other agencies need to be involved.

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



7.3 Bullying

Online bullying should be treated like any other form of bullying and the school anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

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

7.4 Sexual violence and harassment

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 also a document in its own right. It would be useful for all staff to be aware of the DfE guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

The following is an excerpt from section 46 on page 21 of that document:

> *"As with all safeguarding concerns, it is important that in such instances staff take appropriate action in accordance with their child protection policy. They should not assume that someone else is responding to any incident or concern. If in any doubt, they should speak to the designated safeguarding lead (or a deputy). In such cases, the basic safeguarding principles remain the same, but it is important for the school or college to understand why the victim has chosen not to make a report themselves. This discussion should be handled sensitively and with the support of children's social care if required. There may be reports where the alleged sexual violence or sexual harassment involves pupils or students from the same school or college, but is alleged to have taken place away from the school or college premises, or online. There may also be reports where the children concerned attend two or more different schools or colleges. The safeguarding principles, and individual schools' and colleges' duties to safeguard and promote the welfare of their pupils and students, remain the same. The same principles and processes as set out from paragraph 48 will apply. In such circumstances, appropriate information sharing and effective multi-agency working will be especially important."*

8 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, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.
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.

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

9 Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Richmond upon Thames School community. These are also governed by school Acceptable Use Policies and behaviour for learning policy.
Breaches will be dealt with in line with the school behaviour for learning policy (for pupils) or code of conduct (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, The Richmond upon Thames 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.

10 Data protection and data security

NB – the previous version of this policy template included more detail on data protection and security; this August 2018 version is deliberately more concise to avoid conflict or duplication with the full documentation set drawn up in the light of the Data Protection Act 2018 (the UK's implementation of the General Data Protection Regulation, or GDPR). 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' (April 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.*** *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****."*

All pupils, staff, trustees, volunteers, contractors and parents are bound by the school's data protection policy and agreements, which can be found **here**.
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: Sophos Anti-Virus, Egress and Meraki Mobile Device Management.

The Head Teacher, data protection officer and trustees 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.
In the light of GDPR, policies for these areas is clear in data-protection documentation:

- CCTV
- Password policy
- Reminders to lock devices when leaving unattended
- Device encryption
- Access to and access audit logs for school systems
- Backups
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies
- BYOD
- Wireless access

- File sharing
- Cloud platform use, access and sharing protocols

12 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.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

- At the Richmond upon Thames School, we have decided that option Active/Pro-active technology monitoring services is appropriate because allows the school to understand how services are performing, along with identifying potential areas of risk in real-time.

13 Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

13.1 Email

- KS3 students only receive notification emails from classroom.google.com
- Other email communication for students is not yet enabled to ensure better-monitored and more transparent communication within classroom.google.com
- Staff at this school use the **school's Education Google Mail domain** for all school emails

General principles for email use are as follows:

- The only means of electronic communication to be used between staff and pupils / staff and parents (in both directions) is by the **school's Education Google Mail domain**. Use of a non-rts email account must be approved in advance by the Head Teacher. 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 Head Teacher (if by a staff member).

- There should be no circumstances where a private email is used to communicate with parents or students - if this happens by mistake, the DSL should be informed. The DSL may refer this to the Headteacher or DPO, depending on the incident
- The Google Classroom chat is different to Gmail
- Education Gmail is managed by the school and is not the same as a private Gmail account
- Staff or pupil personal data should never be sent, shared or stored on email
    - If personal data needs to be shared with external agencies, a secure service must be used. If in doubt, speak to the Data, Systems and CS lead.
    - Internally, staff should use Google Classroom to communicate with individual or groups of students
- Pupils in Year 7 and 8 will receive emails about announcements posted in Google Classroom but will not be able to send or recieve any other emails.
- 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 will only receive emails from Google Classroom notices and messages. The sending and receiving of all other email is not allowed by students. Staff should report any breaches in this GMail-Student setting, using the ClickOn IT ticketing system.

See also the social media section of this policy.

14 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 Head Teacher and Trustees have delegated the day-to-day responsibility of updating the content of the website to **the Head Teacher's PA.** The site is managed by / hosted by Haymarket Media Group *[from December 2018 E 4 Education].*

The RTS website's LGfL RAG-rating will be attached in the appendix.

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

- RTS 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. If in doubt, check with Deesh Grewal. 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). RTS 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).

15 Cloud platforms: GSuite, Progresso, Meraki, accounts, Inventry, WisePay, NRS Till system

Staff should work towards a culture of safe-working practices and develop a strong awareness of the consequences to the subject and RTS of personal data-loss or breach.

"Take care of the data as if it were your own"

RTS 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. The companies we use to provide these services will already be used at other schools, have a strong commitment to data security and ensure compliance with current data protection regulations. It is important to consider data protection before adopting a cloud platform or service – see our DP policy here

When using these services, staff will be issued passwords which may allow access to personal student or staff data. Therefore staff must ensure good security habits:

- ensure a password of at least 8 characters and a combination of symbols, numbers and capitals
- set different passwords for different services, unless google-log-in has been enabled for that service
- never leave a logged-in device unattended, unless locked physically and
- never share a password but if you do have to, change it immediately after the event
    - For online safety, basic rules of good password hygiene "*Treat your password like your toothbrush –never share it with anyone!*"
- never keep downloaded personal data on your computer hard-drive eg Desktop, Downloads, Documents
- Ensure the physical security of your staff laptop, both on and off the school site
- Ensure no passwords are written down and stored in an accessible location

The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is 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 to be setup for staff with the highest levels of access to the RTS IT systems
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students 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)

16 Digital images and video

When a pupil/student 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 the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication
- For social media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest entry in Progresso 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 The Richmond upon Thames School, members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to Google storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the Google Drive or Google Photos 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 also taught to consider how to publish for a wide range of audiences which might include trustees, 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.

17 Social media (SM)

17.1 The Richmond upon Thames School's SM presence

The Richmond upon Thames 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.

Belinda Campbell is responsible for managing our Twitter/Facebook accounts. She follows the guidance in the LGfL / Safer Internet Centre online-reputation management document here.

17.2 Staff, pupils' and parents' SM 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 should be followed. School complaints procedure policy here.

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/students 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). It is encouraging that 73% of pupils (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

The school has an official Facebook / Twitter / Instagram account (managed by **Head Teacher's PA and Mrs J Marker)** and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils (see page for full details).

Students are not allowed* to be 'friends' with or make a friend request** to any staff, trustees, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, 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.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head Teacher, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head Teacher (if by a staff member).

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) and permission is sought before uploading photographs, videos or any other information about other people.

18 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.

18.1 Personal devices and bring your own device (BYOD) policy

- **Students** are not allowed to have mobile phones enabled devices on their person anywhere on the school site. Mobile phones should be switched off in lockers. Any attempt to use a phone or non-school issued internet enabled device on the school site without permission or to take illicit photographs or videos will lead to confiscation of the device [see the school Behaviour Policy and the school's guidance on mobile phones us in school], the withdrawal of mobile privileges. In come cases, the use of prohibited digital devices will lead to further sanctions. 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 not use their mobile phones for personal use, whilst around students. Some staff may find it easier to take the register on their phone, because Progresso is cloud-based. If this is the case, staff must ensure appropriate security on their phones, in case the phone is lost, stolen or breached.
    - Student or staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, trustees** should keep their phones out of sight e.g. in pockets or briefcases. To take a call, they must move to a location away from the presence of children. 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 Head Teacher should be sought (the Head Teacher may choose to delegate this) and this should be done in the presence of a member of RTS staff.
- **Parents** are asked to keep their phones out of sight e.g. in pockets or bags and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and under no circumstances are they permitted to capture photos of other children.
    - When at school events, please refer to the Digital images and video section of this document on page 16, and parentfilming.lgfl.net may provide further useful guidance]. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. Students are not allowed to use their phones or have them out whilst on the school site.

18.2 Network / internet access on school devices

- **Students** are allowed internet access for educational-use, using school-sanctioned software, services and apps. All use must be in line with the acceptable use policy. All such use is monitored. All infringements will be dealt with in line with the RTS behaviour for learning policy
- **Volunteers, contractors, trustees** can access the guest wireless network and will only have access to the systems and services they are authorised to access. All internet traffic is monitored. Any contractor must be authorised entry to the site in line with the safeguarding and child-protection policy.
- **Parents** have no access to the school network or wireless internet on personal devices.

18.3 Trips / events away from school

Staff may use their personal mobile phones for communication, emergencies and image, sound or video-capture. If such use of a personal device is made:

- photos must only be taken of students for whom parents have given such consent
- staff must ensure they are aware of students who are not allowed to be photographed because their parents have not consented
- the files must be set to import to the RTS Google Photos or Google Drive folders
- the phone should be set to delete these images after upload
- sharing trip-images must be via the school social media platforms and website only

Staff should work towards a culture of safe-working practices and develop a strong awareness of the consequences to the subject snd RTS of personal data-loss or breach.

"Take care of the data as if it were your own"

18.4 Searching and confiscation

In line with the DfE guidance *Searching, screening and confiscation: advice for schools*, the Head Teacher 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.

Full details of the school's search procedures are available in the school Behaviour Policy.

Appendices

1. Safeguarding Incident log [online-safety incidents are logged in the same way as any other safeguarding incident – Provision Map here]
2. Safeguarding and Child Protection Policy here
3. School's Behaviour Policy
4. School's Anti-Bullying Policy
5. School's Staff Code of Conduct
6. School's Staff Handbook
7. School's Acceptable Use Policies (AUPs) for:
    - Simplified version for Year 7 students, focussed on iPads
    - Staff
    - Volunteers, trustees & Contractors
    - *Parents
8. Letter to parents about filming/photographing/streaming school events
9. Prevent Risk Assessment Template
10. Online-Safety Questions from the Governing Board (UKCCIS)
11. Education for a Connected World cross-curricular digital resilience framework (UKCCIS / UKCIS)
12. Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
13. Working together to safeguard children 2018 (DfE)
14. Searching, screening and confiscation advice (DfE)
15. Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
16. Sexting guidance from UKCCIS
    - Overview for all staff
    - Full guidance for school DSLs
17. Prevent Duty Guidance for Schools (DfE and Home Office documents)
18. DfE press release (19 July 2018) – 'New relationships and health education in schools'
19. School's Data protection and data security advice, procedures etc
20. Preventing and tackling bullying (DfE)
21. Cyber bullying: advice for headteachers and school staff (DfE)
22. Statutory requirements of school websites
23. Appendix 1 - Confirmation of Receipt of the school Online Safety Policy

Confirmation of Receipt of the school Online Safety Policy

Name:

Date of joining school:

Post:

Date of induction:

Name and designation of member of staff responsible for induction:

I confirm that I have reviewed and read the school Online Safety Policy.

Signature:

Name:

Date:

Please sign and return this form to the Designated Safeguarding Lead.