St John's C of E (VA) Primary School
LGfL School Online Safety Policy

Date: Autumn 2019
Frequency of review   1 year
Reviewed by   Personnel

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety <u>must</u> follow the school's safeguarding and child protection processes.

Contents

1. Introduction and Overview
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy is communicated to staff/pupils/community
   - Handling complaints
   - Reviewing and Monitoring
2. Education and Curriculum
   - Pupil online safety curriculum
   - Staff and governor training
   - Parent awareness and training
3. Expected Conduct and Incident Management
4. Managing the IT Infrastructure
   - Internet access, security (virus protection) and filtering
   - Network management (user access, backup, curriculum and admin)
   - Passwords policy
   - E-mail
   - School website
   - Learning platform
   - Social networking
   - Video Conferencing
5. Data Security
   - Management Information System access
   - Data transfer
   - Asset Disposal
6. Equipment and Digital Content
   - Personal mobile phones and devices
   - Digital images and video

Appendices
   Appendix A: Acceptable Use Agreement (Staff, Volunteers and Governors)
   Appendix B: Acceptable Use Agreements (Pupils – KS1)
   Appendix C: Acceptable Use Agreements (Pupils – KS2)
   Appendix D: Acceptable Use Agreement including photo/video permission
                  (Parents)

Updated: November 2016

© London Grid for Learning (www.lgfl.net)

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at St. John's with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of St. John's community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the school's IT systems, both in and out of St. John's.

Roles and responsibilities

Role	Key Responsibilities
Headteacher/ Deputy Head Teacher	- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance - Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles

Updated: November 2016

Role	Key Responsibilities
	• Be aware of procedures to be followed in the event of a serious online safety incident • Ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • Ensure school website includes relevant information.
Designated Child Protection Lead	• Lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • Take overall responsibility for online safety provision • Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • Liaise with school technical staff where appropriate • Communicate regularly with SLT and the safeguarding governor Governor to discuss current issues • Ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • Ensure that online safety incidents are logged as a safeguarding incident • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/ Safeguarding governor (including online safety)	• Ensure that the school has in place policies and practices to keep the children and staff safe online • Approve the Online Safety Policy and review the effectiveness of the policy • Support the school in encouraging parents and the wider community to become engaged in online safety activities • Meet regularly with Designated Child Protection Lead
Computing Curriculum Leader	• Oversee the delivery of the online safety element of the Computing curriculum
IT technician (provided by Open Air services)	• Ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services • Report online safety related issues that come to their attention, to the Designated Child Protection Lead • Manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices

Updated: November 2016

© London Grid for Learning (www.lgfl.net)

Role	Key Responsibilities
	- the school's policy on web filtering is applied and updated on a regular basis • That they 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 • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Designated Child Protection Lead/Headteacher • Ensure appropriate backup procedures and disaster recovery plans are in place
Office Manager	• Take overall responsibility for being the Data Protection Lead in the school, ensuring school's provision follows best practice in information handling • Ensure that the data the office overseas is accurate and up-to-date • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner
LGfL Nominated contact(s)	• Ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	• Embed online safety in the curriculum • Supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff,	• Read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • Report any suspected misuse or problem to the online safety coordinator • Maintain an awareness of current online safety issues and guidance e.g. through CPD • Model safe, responsible and professional behaviours in their own use of technology Exit strategy • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset. Their accounts would be deleted or if a general login used then the password would be reset
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Policy at the beginning of Key Stage 1 and Key Stage 2 • 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

Commented [L1]: Data Protection Lead

Updated: November 2016

Role	Key Responsibilities
	• Understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • Contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• Read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren • Consult with the school if they have any concerns about their children's use of technology • Support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.
- Reference to the policy/ online safety links will be included as appropriate in newsletters.

Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements and possible sanctions.
- Designated Child Protection Lead acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to the Designated Child Protection Lead as soon as possible
- Any concern 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 Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - o Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?

Updated: November 2016

© London Grid for Learning (www.lgfl.net)

- o Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- o Are there any adults involved in the sharing of imagery?
- o What is the impact on the pupils involved?
- o Do the pupils involved have additional vulnerabilities?
- o Does the young person understand consent?
- o Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Child Protection policy and Anti-Bullying policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- regularly revisits online safety education throughout the year and through termly 'Be Safe' weeks
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, appropriate use of devices, research skills, copyright;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes training available to staff on online safety issues;
- provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school makes parents/carers aware of online issues by

- publishing relevant articles in the school newsletter as appropriate
- holding information evenings
- circulating relevant materials from external publishes (digital parenting)

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;

- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors
- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers
- should provide consent for pupils to use the Internet, as part of the online safety acceptable use agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

Incident Management

In this school:
- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering
This school:
- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). Any changes to the filtering policy are made by the IT technicians after being advised by the Head Teacher or Deputy Head Teacher.
- uses USO user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);

Updated: November 2016

- Uses DfE, LA or LGfL approved systems including DfE S2S, LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices (USBs) or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)
This school
- Uses individual, audited log-ins for all adult users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school data (admin and curriculum);
- If required will use secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, this school:
- Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, username and password. The same credentials are used to access the school's network.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off or lock their computer when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies;
  e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;

Updated: November 2016

- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy
- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords into the MIS, LGfL USO admin site, every 90 days/twice a year.
- We require staff using critical systems to use two factor authentication.

E-mail
This school
- Provides staff with an email account for their professional use, London Staffmail and makes clear personal email should be through a separate account;
- Where appropriate we use anonymous or group e-mail addresses, for example office@st-johns.croydon.sch.uk or class e-mail addresses.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses.

Pupils:
- We use LGfL pupil email system which are intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:
- Staff will only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked

School website
- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing

Updated: November 2016

to the school website; permission form parents is explicitly sought before using a child's image on the school website

Social networking
Staff, Volunteers and Contractors
- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- for the use of any school approved social networking will adhere to school's social media policy.

School staff will ensure that in private use:
- No reference should be made in social media to pupils, parents/carers or school staff or any school related matters;
- School staff should not be online friends with any pupil. If a pupil tries to contact a member of staff using any form of social media the member of staff should report this to the staff should report this to the online safety co-ordinator.
- Staff do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:
- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our Key Stage 1 and Key Stage 2 pupil Acceptable Use Agreement (as age appropriate).

Parents:
- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required. (see Appendix E)
- Are reminded that they should not uploading photographs, videos or any other information about other children to social media.

5. Data security: Management Information System access and Data transfer
Strategic and operational practices
At this school:
- The Office Manager is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

Updated: November 2016

Technical Solutions
- Staff have secure area(s) on the network to store sensitive files.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are managed by DBS-checked staff.
- Details of all school-owned hardware is be recorded in a hardware inventory (the school asset register).
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where appropriate any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)
- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff should only use mobile devices in places where children are not present (offices, staffroom, empty classroom).
- Staff (and parents/carers on a school outing) should not take any images/video of children or download any images using their own personal devices. For public events such as school plays, Sports day parents/carers are permitted to take images using their own devices as long as they are only for their own personal use and they are not shared/used online
- Mobile devices are not permitted to be used in certain areas within the school site (refer to mobile phone policy for further details).
- Older pupils are only permitted to bring a personal mobile device into school if they and their parent/carer has signed the mobile phone protocol. Phones which are brought into school, must be turned off (not placed on silent) and placed in the class mobile box which is stored securely in the office until the end of the day.
- Staff members may use their phones during school break times as long as they are in designated areas where children are not present.
- All visitors are requested to keep their phones on silent and to not use them while they are on the school property.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Updated: November 2016

© London Grid for Learning (www.lgfl.net)

Storage, Synching and Access
School devices accessed with a school owned account
- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

School devices accessed with a personal account
- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Digital images and video
In this school:
- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes not using mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school website in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- 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 governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. 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.

Appropriate use of Social Network Sites and Apps

The school has an expectation that all parents will model appropriate use of social media use so that any concerns are made through the appropriate channels and in accordance with school policy - by speaking to the class teacher, the Head teacher or the Chair of Governors, so they can be dealt with fairly, appropriately and effectively for all concerned.

Anyone using social media must remember that, when making a post, they have not only their own reputation to consider but also that of others and that of the School. Every member of the school community has to take responsibility for their own actions when online and is expected to demonstrate high levels of professionalism and good judgement at all times.

As a school we are aware that social media websites are being used increasingly to fuel campaigns and complaints against schools, Head teachers, school staff, parents and pupils. The Governors of St John's considers the use of social media websites being used in this way as unacceptable and not in the best interests of the children or the whole school community.

Anyone using social media should be aware that once something is posted online in the digital realm, it has a persistence that is not like something that is said. It is replicable and searchable, and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context.

All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this. In the unlikely event that any parent/carer of a child/ren at St John's is found to be posting or sharing unkind, libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the relevant network site.

This approach will be shared with parents through the home school agreement.

Updated: November 2016