Policy Document:	ICT AND ONLINE SAFETY POLICY
School's Lead Member of Staff:	DSL supported by Head Teacher
Lead Governors (monitoring):	FULL GOVERNORS
Publication/Revision Date:	February 2022
Document Version:	1.4
Governor Committee:	FULL GOVERNORS
Committee Approval Date:	February 2022
Full Governors Ratification Date:	January 2022
Review Frequency:	2 Years
Date of next review:	February 2024
Publication Date:	February 2022
Purpose:	To ensure that online safety is clearly viewed as part of the school's statutory safeguarding responsibilities and that the DSL and Headteacher actively promote safe and responsible use of digital information and communication within the school.

Chair of Governors signature:

ICT and Online Safety Policy

This document should be read in conjunction with the school's Safeguarding policy.

Contents

ICT & ONLINE SAFETY POLICY DEVELOPMENT PROCESS AND STAFF TRAINING

Policy development

This Online Safety policy has been developed as a collaborative document involving input from:

- Safeguarding team
- Governor responsible for Safeguarding
- Head Teacher & Principal
- Senior Leadership Team, including SENDCO, Heads of School and Head of Communications/Operations
- Staff – including teachers, support staff, technical staff
- Chair of Governors and full Governing body
- Student Council

The policy has been informed by the following DfE guidance for schools and from School Improvement Liverpool :

Keeping children safe in education 2021

Safeguarding and remote education during coronavirus (COVID-19)

School Improvement Liverpool's Online safety updates for DSLs and Headteachers

Guidance and templates provided by the Southwest Grid for Learning and the London Grid for Learning have been used.

Schedule and Procedures for Monitoring & Review

The implementation of this Online Safety policy will be monitored by:	The Senior Leadership Team with guidance from the DSL, Head Teacher and Principal.
Monitoring will take place at regular intervals:	Formally at least once a year, although more frequent informal monitoring will take place termly
The Governors will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	At governors 'meetings at least once a year
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	December 2022
Should a serious online safety incident take place involving a child, the following external agencies should be informed:	*Police*
Should a serious online safety incident take place involving an adult, the following external agencies should be informed:	*LADO* *Phil Cooper (School Improvement Liverpool)*

Monitoring procedures

The school monitors the impact of the policy using:

- Logs of reported incidents
- Surveys / questionnaires completed by:
    - pupils
    - staff
    - parents / carers
- Learning walk and report by Governor with safeguarding responsibility
- Logs of filtering blocks through which we can identify when and which group of students might be involved in accessing unsuitable material.

Scope of policy

This policy applies to all members of the CFS school community, including staff, pupils, volunteers and parents/carers who have access to and are users of the school's digital technology systems, both in and out of the school. The policy also applies to visitors to the school who have access to or use the school's digital technology systems.

The Education and Inspections Act 2006 imposes a duty on the school to regulate (to such extent as is reasonable) the behaviour of pupils when they are off the school site, and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other online safety incidents that occur outside of school when they are linked to membership of the school. The 2011 Education Act empowers the school to search for electronic devices and to view and delete their content where this is in contravention with the school's Behaviour Policy. The school will deal with such incidents in line with this policy and our associated Behaviour and Anti-bullying policies. Where known, the school will inform parents/carers of incidents of inappropriate online behaviour that takes place out of school.

Roles and responsibilities

1. **Governors**

   Governors are responsible for ensuring that:

   - holding online safety is a running and interrelated theme in all relevant policies
   - online safety is considered in curriculum planning, staff training and parental engagement
   - appropriate filters and monitoring systems in place
   - appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners from cyber-crime, periodically reviewing the effectiveness of these procedures

   Governors are also responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

   A member of the Governing Body (Jenny Oliver) has responsibility for Online Safety as part of her overall Safeguarding remit.

   The role of the Governor with responsibility for online safety involves:

- holding regular meetings with key staff responsible for online safety (Principal, Head Teacher and DSL)
- regular monitoring of online safety incident logs/reports
- reporting to Governors at regular intervals

Governors will receive information about online safety incidents and regular monitoring reports.

2. Online safety senior leadership team

At CFS, the Principal, Head Teacher and DSL all have expertise in aspects of online safety, so can work together effectively as an online safety leadership team.

The Head Teacher and Principal have a duty of care for ensuring the safety (including online safety) of members of the school community, working closely with the DSL in her role as online safety lead.

The Head Teacher and Principal are responsible for ensuring that the DSL (in her capacity as online safety lead) and other relevant staff receive suitable training about the unique risks to children online so that they are enabled to carry out their roles and to train other staff. This should include training about the additional risks that children with special educational needs and disabilities (SEND) face online - for example, from online bullying, grooming and radicalisation - and how to support children with SEND to stay safe online.

The Head Teacher and Principal in collaboration with the DSL (as online safety lead) will ensure that there is an effective system in place to monitor online safety throughout the school.

The Head Teacher, Principal and DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.

3. DSL in her capacity as Online safety lead

CFS recognises that online safety is part of the school's overall safeguarding responsibilities. Digital technologies provide additional means for safeguarding issues to develop but they are not different in kind from safeguarding concerns that develop in other contexts. For this reason, we have chosen to combine the role of DSL and online safety lead.

The DSL in her capacity as online safety lead is trained in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from: sharing personal data, access to illegal or inappropriate materials, inappropriate contact with adults/strangers, potential or actual incidents of grooming and online bullying.

The DSL in her capacity as online safety lead will work **collaboratively with** the Head Teacher and Principal to:

- review the school's online safety policies and documents
- advise on methods of monitoring online safety
- review reports from staff about online safety incidents with a view to ensuring that any lessons learnt will inform future online safety developments
- inform the governor responsible for safeguarding about any significant online safety issues/developments and include updates about our online safety policy and procedures in safeguarding reports to governors
- consult with other members of the SLT about the implementation of the online safety policy through the school
- oversee the provision of training and advice for staff
- ensure that any relevant information from School Improvement Liverpool about online safety concerns/alerts is disseminated to staff, pupils or parents as appropriate
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- seek advice from SIL about how to respond to serious online safety incidents in school.
- liaise with staff (especially teachers, support staff, the ICT technician, the mental health lead and SENDCO) on matters of online and digital safety and when deciding whether to make a referral to relevant external agencies so that children's needs are considered holistically.

4. Network manager and technician

The Principal in conjunction with the school technician are responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements
- users may only access the school's network, Google platform and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- the use of the school network, internet and other digital technologies is regularly monitored so that any misuse or attempted misuse is reported to the Head Teacher, DSL (in her capacity as online safety lead) and other relevant SLT members
- monitoring systems are implemented and updated as agreed in school policy.

5. Teaching and support staff, including volunteers

All teaching and support staff (LSAs, TAs or 1:1 support workers) are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff and volunteer acceptable use agreement
- they report any suspected misuse of problem to the Head Teacher or Principal or DSL (in her capacity as online safety lead) for investigation and further action
- all digital communications with pupils, parents and carers are conducted in line with school policy
- pupils understand and follow the school's Acceptable Use Policy for pupils - Middle and Upper School pupils are expected to sign and follow the written version of this policy; relevant aspects of the policy are explained to Lower School pupils orally
- they monitor the use of digital technologies in lessons and other activities, including the use of computers, Chromebooks, cameras, tablets/ipads, pupil's own laptops or mobile phones (where allowed) and implement current policies and procedures
- they put into action agreed processes for dealing with any unsuitable material that is found in internet searches [see section 2.1.1.4]

For teachers specifically:

- they ensure that online safety issues are embedded in the curriculum and other activities as appropriate
- pupils have a good understanding of online research skills and the need to avoid plagiarism and uphold copyright regulations
- in lessons where internet use is pre-planned, teachers should generally guide pupils to sites that have been checked as suitable for their use, although as pupils move up the school it is expected that they will be given more opportunities to undertake their own research within parameters set by the teacher.

6. Pupils

Pupils are responsible for:

- using the school digital technology systems in accordance with the pupil acceptable use agreement, including the use of mobile phones, cameras and wearable devices and the taking/sharing of images
- applying the research skills they are taught to avoid plagiarism and uphold copyright regulations
- reporting abuse, misuse or access to inappropriate material, using appropriate channels
- following good online safety practices when using digital technology not only in school but also when out of school, recognising that the school's online safety policy covers their actions outside of school if it relates to their membership of the school
- recognising what constitutes online bullying and knowing how to take action to stop it through reporting and other measures.

7. Parents/carers

As part of our distinctive character as a parent collaborative school, we recognise and acknowledge the crucial role that parents/carers play in helping their children navigate the digital and online world. In keeping with our school commitment to support parents in fulfilling their 'parental mandate', we place great importance on training and equipping parents to be effective educators of their own children about online safety. This is done through material made available on our website and other school communications, as well as through

bi-annual parent education events and at transition meetings (entering Lower School, moving into Middle School, going into Upper School). The material we share with parents includes a parent copy of the pupil acceptable use agreement at induction and at the start of each school year, samples of online safety education materials used in school, as well as appropriate and relevant information for parents, generated by nationally recognised online safety experts.

Parents are asked to follow guidance from the school about the appropriate use of pictures taken at school events.

8. Online safety collaborative group

The development and implementation of an effective online safety policy requires consultation with and support from a wide range of stakeholders in the school, including staff, pupils and parents/carers. We have regularly consulted with all three groups of stakeholders and have trained each group separately.

We are setting up an online safety group with the specific task of exploring the feasibility and value of using the 360^{0}Safe online safety self-review tool to review our online safety policy and practice. Overview of the Tool | 360safe

The 360^{0}Safe tool is intended to provide information that will enable us to identify strengths and weaknesses in our current policy and practice and further strengthen both. A key question is whether this tool supplements or duplicates the 175 audit we currently use to review our overall safeguarding practice and whether any supplementary information adds significantly to our understanding of the online safety of pupils and staff in school. The group will comprise the DSL, the Principal, the Head Teacher, a representative from the Student Council, a representative from the staff body and a parent representative.

CFS ONLINE SAFETY POLICY STATEMENTS

1. Guiding principles

1.1 PUPILS NEED TO BE KEPT SAFE

We fully accept our responsibility to actively promote safe and responsible use of digital communication within our community.

1.2. PUPILS NEED ADULT GUIDANCE

We recognise that some safeguards which have the desirable aim of protecting children/young people from predatory adults may prevent them being overseen by safe adults. We do not support the creation or development of adult-free, private zones for children/young people, either on- or off-line where their activity cannot be subject to age-appropriate adult guidance and discipline.

1.3. INTEGRITY IN MULTIPLE ROLES

It is recognised that in a digital age, staff and many pupils (principally those in Middle and Upper School) will have an online life that intersects with the rest of their life, both in and out of school.

In a Christian community, it is expected that all members will strive for personal integrity in all aspects of their lives, so that their online life and character is in keeping with their off-line life and character both in and out of school.

"Whatever you do, in word or deed, do all in the name of the Lord, giving thanks to God through him."

The close-knit nature of our community, where members may have multiple modes of relationship with one another – as relatives, friends, fellow church members, colleagues, classmates, teacher/pupil – poses both opportunities and risks.

All members of the school, whether staff (paid and voluntary), parents, students and friends, have a responsibility to conduct themselves on-line in a way that maximises the opportunities for positive relationships and minimises the risks.

Staff (paid and voluntary) have additional responsibilities in line with statutory and school obligations for safeguarding and protecting children.

2. ONLINE SAFETY EDUCATION

2.1 PUPILS

2.1.1 Online safety across the curriculum

The school is actively committed to ensuring that online safety is a focus across the curriculum. Our objective is an online safety curriculum that is broad, relevant and provides progression, with opportunities for creative and reflective activities.

Our online safety curriculum covers a wide range of issues covering four key areas of risk:

- CONTENT - being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism

- CONTACT - being subjected to harmful online interaction with other users; including: peer-on-peer abuse, peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- CONDUCT - personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online (cyber) bullying

- COMMERCE - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

We recognise that a one-size-fits-all approach is not always appropriate, so we may as appropriate adopt a more personalised or contextualised approach for more vulnerable children e.g. SEND or victims of abuse.

2.1.2 Online safety teaching and learning methods

It is essential that children are safeguarded from potentially harmful and inappropriate online material. We have a whole school approach that protects and educates pupils, students, staff and parents in their use of technology and has established mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The school uses a variety of methods of providing this online safety education and staff reinforce online safety messages in a range of relevant contexts, including:

- A planned online safety curriculum delivered in all key stages through PSME lessons (RSE and safeguarding strands) about using digital opportunities safely and responsibly
- Form tutor sessions in Lower, Middle and Upper School
- Special age-appropriate assemblies, usually focused around Safer Internet Day themes
- as part of collapsed timetable activities
- as part of the iDEA badge award work undertaken by Upper School pupils in the context of ETS
- in Computing lessons.

Pupils are taught across the curriculum to be critically aware of the materials and content they access online and be guided to validate the accuracy of information. When presenting material, pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed through the internet.

As part of our duty under the Counter-Terrorism and Security Act 2015, pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

We recognise that from time to time, for good and valid educational reasons, pupils may need to research topics (such as racism, drugs or terrorism) that would normally result in internet searches being blocked. In such situations, staff may request that the ICT technical support staff can temporarily remove these sites from the filtered list for the period of study. These requests must be in writing, with clear reasons given for the need and a time limit indicated so that the blocks can be reinstated afterwards.

Pupils will also be taught at age-appropriate stages about cyber crime. This will include an understanding that cyber-enabled or cyber-dependent crimes include unauthorised access to computers (illegal hacking) such as accessing a school's computer to look for test paper or alter a grade; denial of Service (Dos or DDoS) attacks; and making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offences.

If pupils with particular skill and interest in computing and technology inadvertently or deliberately strays into cyber-dependent crime, the DSL or her deputy should consider referring the pupil to the Cyber Choices programme: Cyber Choices: Helping you choose the right and legal path - National Crime Agency This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests. The Cyber Choices programme does not cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs, child sexual abuse and exploitation, which are higher level offences and should be referred to the local police.

2.1.3 **Training in personal responsibility**

We recognise that whilst regulation and technical solutions are very important in keeping pupils safe, this must be balanced by educating pupils to take a responsible approach themselves. This is supported by evidence of the relative safety of pupils in 'locked down' versus 'managed' systems.

The school has regard to the duty of governing bodies and proprietors to ensure that appropriate filters and monitoring systems are in place, but take account of the guidance in Keeping Children Safe in Education that "they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding." (KCSIE, 2021) We note that "pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves." OFSTED, 2010.

The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

2.1.4 **Online safety during remote education under COVID 19 pandemic regulations**

Our remote education safeguarding policy and procedures are informed by DfE guidance on Safeguarding and remote education during coronavirus (COVID-19) and the SWGL's Safe Remote Learning advice.

2.1.4.1 The school will provide **remote education** to pupils when, in accordance with government guidance or legislation around coronavirus (COVID-19), a class, group or a small number of pupils need to self-isolate, or local restrictions mean that pupils are to remain at home. Remote education could be delivered by a variety of means: assignments set on Google Classroom, education materials sent home or Google Meets. Where Google Meets are used, it is preferable for the Form Tutor to set up one Meet for the whole day, inviting all subject teachers, rather than individual teachers setting up Meets. A Chromebook with the Meet already open can then be carried from lesson to lesson.

All such pupils who are not physically unwell will have access to remote education as soon as reasonably practicable, usually the next school day. The school aims to make our remote education provision as safe and high quality as in-school provision. The school has been able to move swiftly to remote education due to our established experience with Google Suite for Education in normal circumstances.

2.1.4.2 Keeping pupils, students and teachers safe during remote education is essential. Staff delivering remote education online should be aware that the same principles set out in the school staff code of conduct will apply when working remotely with pupils online.

Key principles for maintaining a safe environment when working remotely online include:

- Clearly communicated **behaviour expectations** for both staff and pupils, such as when cameras should be on and when they can be turned off and whether pupils can use chat facilities during the online lesson.
- Clear processes for **reporting** concerns
- Clear **data protection** procedures

Our safeguarding responsibilities and duties during a period of school is set out in this document shared with all teaching and support staff: CFS Safeguarding actions in response to coronavirus school closure

2.1.4.3 **Online lessons using Google Meet**

Teachers are advised that when delivering a live online lesson they should have regard to the need to project a **professional image** even from home. This means that teachers should be dressed appropriately and should be standing

or sitting upright at a table or desk, not lounging on a bed or sofa. Teachers should have regard for the background of the room and ensure that they do not have inappropriate objects or personal information on view. This is to protect their personal and professional reputation, as well as the reputation of the school.

The general expectation is that **pupils' cameras** should be on during interactive sections of an online lesson but may be turned off at other times. This is because teachers teach better if they have non-verbal cues from pupils about their response to the lesson material.

- We recognise that some pupils find it challenging to have their camera on due to social anxiety, self-consciousness and fear of what others will be thinking when they are on camera. Whilst maintaining our general policy of 'cameras on' for interactive sessions, we will work with pupils and parents to make **reasonable adjustments** where there are clear indications that the policy would adversely affect these pupils' learning. Pupils will be able to turn off their cameras only if special permission has been granted from the ALPS department.

- Some research has suggested that not being appropriately dressed is one of the main reasons for reluctance to turn cameras on. Our policy would therefore be to **encourage pupils learning at home to get dressed** so they are mentally more in 'learning mode' rather than slopping around in PJs.

- Other pupils may feel embarrassed for cameras to see inside the home. We will encourage and facilitate pupils to use a **virtual or blurred background** or if that is not possible, to ask for parent support to rig up a neutral background at home.

- We recognise that creating a culture of trust and safety will encourage pupils to switch their cameras on willingly. Teachers will look for ways to encourage pupils to feel comfortable about being on camera, including icebreakers and other games that put the focus on the activity rather than the pupil.

- We recognise that some pupils will not have the technology available at home to allow for cameras to be on. Form teachers and heads of school may need to work with families to ascertain if there are ways we can help them with technical support, including the loan of Chromebooks or other equipment. If there are still temporary or permanent technical

difficulties, teachers will be expected to find alternative ways of facilitating these pupils' engagement in the lesson.

To maximise inclusivity, teachers should also make use of the **Chat facility** during sections of lessons that require pupil response. However, teachers will need to set clear expectations that the chat facility, when on, can only be used for clearly **educational purposes.** Pupils should not have access to chat during presentation sections of lessons. It is up to teachers to decide whether to activate chat during sections of the lesson where pupils are working independently on material. It can be useful to get immediate feedback from pupils about problems and pupils can be trained to use it productively to provide peer support.

Only CFS staff are able to **set up Google Meets** using school accounts; pupils do not have this facility enabled. Staff are asked to disable Guests being able to add other people to the Meet. This is to prevent people from outside the school community being added without staff being aware. Staff are advised to check carefully that people on the Meet are all members of the school community and that a guest with an external account has not been added.

Pupils are not allowed to re-purpose staff-initiated Meets for unsupervised/ unmonitored social communication purposes. To reduce the opportunity for pupils to **re-use Google Meets**, staff are advised to remove the Google Meet video conferencing facility after the Meet has concluded. It is important that staff do not delete the Google Meet from their calendar as there should be a record of when Meets were scheduled.

Google Meet 1:1 sessions: staff should add a second adult (usually a member of staff but could also be a parent) if they are going to undertake 1:1 sessions with an individual pupil. The second adult does not need to be on the Meet for the duration of the session but the fact that a second adult has access to the Meet at any time will provide some safeguarding protection to both the adult and child. Staff should record 1:1 Meets to provide evidence in the event of any allegation of misconduct although these recordings should not be shared with pupils.

Google Meet recordings: Only CFS staff are able to record Google Meet sessions; pupils do not have this facility enabled. Before recording the Meet session, staff should check that all participants are happy for the session to be recorded. Recordings of Google Meets that are shared with pupils should be kept for the minimum amount of time possible afterwards, generally only long enough for pupils to use for immediate study purposes. 1:1 Meets should be

kept in the teacher's Google Drive area so there is a record of the Meet in the event of any future concern being raised. Pupils are not allowed to share Google Meet recordings on any platform without the explicit permission of an appropriate member of staff.

2.1.4.4 **Reporting concerns**

Staff who encounter an online safeguarding incident or have a concern about a potential breach of the school's online safety policy by pupils or staff in the context of remote learning, should use the same reporting procedures as in normal times.

It is very important that during a period of remote learning, staff are as vigilant as possible about changes in pupils' demeanour and behaviour during online lessons or 1:1 sessions, as this might be the primary way in which children in need of further support or interventions can be identified and helped. Any concerns about a pupil's wellbeing should be reported using the digital version of the referral form.

2.2 Staff and volunteer training

All new staff and volunteers should receive online safety training as part of their **induction**. New staff and volunteers should receive a copy of this policy with key areas highlighted that are particularly relevant to the type of work they will be doing in school. All new staff have to read and sign the Staff/Volunteer Acceptable Use Agreement which summarises their main responsibilities under this policy.

All staff receive regular online safety training so that they understand in more depth their responsibilities as outlined in this policy. There is a planned programme of **formal online safety training for all staff**, which is delivered as part of our regular safeguarding update training in staff meetings and INSET days. Staff who are unable to attend in person are sent an outline of the content with links to relevant material. This programme is regularly updated and reinforced.

All staff means all staff, not just teaching staff. A child could disclose an online safety concern to any adult, therefore all members of staff should be aware of how to recognise, respond to, record and refer online safety concerns.

All staff are made aware that:

- technology is a significant component in many safeguarding and wellbeing issues
- risks of harm relate to the 4C's: content, contact, conduct and commerce
- children are at risk of abuse online as well as face to face
- in many cases abuse will take place concurrently via online channels and in daily life with technology being used to threaten, encourage or facilitate off-line physical abuse or child sexual exploitation
- children can abuse their own peers online (peer-on-peer abuse) - this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups (including upskirting images), and the sharing of abusive images and pornography (including situations where the child is not immediately aware that videos or images of themselves are being shared)
- consensual or non-consensual sharing of nudes/semi-nudes can be signs that a child is at risk of harm and is a safeguarding issue
- it may be appropriate if staff detect a casual attitude towards peer-on-peer sexual harassment to inform pupils about:
    - the recent Domestic Abuse Act 2021 which makes it a criminal offence not only to expose sexual photos or videos of another person with the intent to cause them distress and without their consent, but also to *threaten* to expose such material, even if in fact the material does not exist

      and/or

    - the Voyeurism (Offences) Act 2019 (commonly known as the Upskirting Act) which makes it a criminal offence to take a picture under someone's clothing (not necessarily a skirt) without their permission or knowledge with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm
- online sexual comments, remarks and jokes may be standalone or part of a broader pattern of abuse
- cyber-bullying can be considered a form of emotional abuse
- initiation or 'hazing' type violence and rituals may also include an online element

- even if pupils are not reporting online abuse in school, it does not mean it is not happening, as pupils may be wary of reporting incidents that have taken place on platforms or gaming websites that adults could consider inappropriate
- staff should be ready to challenge and report any situations where they discover online abuse has taken place - whether in school or outside school - and not downplay it, for example dismissing sexual harrassment as 'banter' or 'just a joke', as this normalises abusive online behaviour
- they should report to the DSL any concerns about pupils who might be engaging in 'low-level' cybercrime behaviour, including illegal hacking or making, obtaining or distributing malware
- how to report online safety concerns using the welfare/safeguarding referral form
- they should not view or forward illegal images of a child, recognising that where they believe a child's device contains indecent/illegal images associated with peer-on-peer abuse, it may be more appropriate to confiscate any devices to preserve evidence and hand them to the police for inspection.

An **audit** of the online safety training needs of all staff will be carried out this year (2021-22) and staff will be facilitated to undertake further training as required. This is necessary to evaluate the effectiveness of the online safety training that staff have received and to pinpoint areas for improvement and development.

Individual staff may indicate the need for further online safety training as part of the **appraisal** process. The staff member's line manager (usually Head of School or Head of Department) will then liaise with the Principal and Head Teacher to decide on the best way to facilitate this.

The online safety lead (DSL) and Head Teacher receive **regular updates** through attendance at external training events organised by School Improvement Liverpool. They also receive digital updates from a range of online safety training providers including UK Safer Internet Centre, ParentZone, ThinkUKnow, and InternetMatters. Relevant information from these sources is passed on to staff in the form of staff briefings and emails or as staff meeting agenda items. The DSL and Head Teacher, with support from the Assistant Head (Operations and Communications) will scan and review guidance relating to online safety from the DfE.

The online safety lead (DSL), Principal or Head Teacher will provide **practical advice, guidance or training** to individuals as required.

2.3 Parent/carers training

At CFS we recognise the primary role that parents have in the education and protection of their children online. However we are also aware that some parents have only a limited understanding of the opportunities, risks and issues facing their children online.

The school will therefore provide information to increase parents' awareness and understanding, including parent forums, parent bulletins and information posted on the website. Tri-annually online safety will be the main focus of a PFC meetings. The school subscribes to ParentZone's *Digital Parenting* magazine which contains highly relevant and clearly communicated information for parents. This is distributed to parents through the brown envelope and a digital .pdf version is sent out via the school email system. Providing information in other community languages represented in the school is an area we are actively researching.

2.4 Governor training

Governors are invited to attend and participate in online safety training sessions put on at school and will receive online safety briefings sent out to parents. Specific online safety training will also be provided by one of the Online Safety Senior Leadership Team.

The governor with responsibility for safeguarding also accesses online safety training provided by School Improvement Liverpool.

3. Technical infrastructure

3.1 SCHOOL INTRANET, FILTERING AND MONITORING

3.1 1 The school's servers, wireless systems and cabling are **securely located**. They will only normally be accessed by the ICT technician, members of the online safety senior leadership team, the site manager and contractors and others working on the electrical/cabling infrastructure.

3.1.2 All users have clearly defined access rights to school systems and devices.

- Staff are provided with a username and secure password on registration as a user on the school system. The ICT technician keeps a record of usernames and passwords. No other person, apart from the Principal, has access to this record. Staff are advised on registration that their school account details are held by the school and their

- Pupils from Y4 onwards are provided with a username and secure password by the ICT technician or Principal, who keeps an up-to-date record of pupils and their usernames and passwords. This record can be accessed by members of the SLT in order to carry out their safeguarding duties and to facilitate easy recovery of forgotten passwords. Users are responsible for the security of their username and password.

- Pupils in Lower School use group logons.

3.1.3 The governing body and proprietor of the school have a statutory duty to do "all that they reasonably can to limit children's exposure to the [four areas of risk] from the school . . . IT system. As part of this process, governing bodies and proprietors should ensure their school or college has **appropriate filters and monitoring systems** in place. Governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty." (Keeping Children Safe in Education, 2021, 128)

The statutory guidelines make it clear that "Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should 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."

3.1.4 The Prevent Duty guidelines state that schools in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing **appropriate levels of filtering**". (Revised Prevent Duty Guidance 2015). The school has adopted filtering and monitoring methods that it considers appropriate in relation to risks, cost and outcomes, drawing on the advice of the UK Safer Internet Centre's about what 'appropriate' looks like. Appropriate Filtering

The school uses the SafeDNS filtering method to prevent users from accessing material online. The SafeDNS system provider is an IWF (Internet Watch) member and blocks access to illegal Child Abuse Images and Content (CAIC). The SafeDNS filtering system screens for and blocks access to material that promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex; displays or promotes the illegal use of drugs or substances; promotes terrorism and terrorist ideologies and violence; promotes the compromising of system by malware or hacking; displays sexual acts or explicit images; includes illegal provision of copyrighted material through piracy or theft; promotes or displays deliberate self-harm (including suicide and eating disorders); displays or promotes the use of physical force intended to hurt or kill.

3.1.3 The school uses four main methods to **monitor pupil activity online** in school and at home when using school-provided facilities:

3.13.1 **Physical observation** of small groups of pupils using computers or other internet-linked devices, by keeping pupils' screens in constant or very regular view throughout a lesson. When pupils are using Chromebooks, they are required to position themselves so that their screens can be seen at all times by the teacher in the classroom.

3.1.3.2 **Veyon (iTALC) classroom management** system which enables staff to regularly check all pupil screens in the ICT room from a central screen on a dedicated computer on the teacher's desk. This is the preferred method to be used in the ICT room unless there are just two or three students whose screens can be seen at all times. Staff who teach or supervise larger groups in the ICT room are expected to ensure that they have the Veyon computer and screen on and can see all the screens of all computers being used during the lesson.

3.1.3.3 **Regular random checks on pupil activity on Google Hangouts** will be carried out by selecting a specific pupil and reviewing the content and tone of their communication on Hangouts and/or Gmail. All pupils and parents have been informed that school Google accounts can and will be monitored.

3.1.3.4 **Parent reporting of concerns** is very important for us as a parent collaborative school. Parents are regularly reminded that they should be monitoring their children's online activity and reporting any concerns to school. Parents are advised that if they have concerns about the content or tone of communications on school-provided platforms or on parent-provided platforms, they should take screenshots to pass on to school (with the exception of indecent images of children, which would constitute a criminal offence).

3.1.3.5 If monitoring leads to the discovery of a pupil contravening the school Acceptable Use of ICT policy, the incident should be recorded appropriately. In Middle School and Lower School this will usually be via the Discipline or Welfare forms. Any disciplinary or welfare issues should be reported to the form tutor and Head of School. If the incident involves any online bullying the matter should be reported to the DSL as well.

A log of reported incidents will be kept, summarising the nature of the incident and the action taken.

3.2 CFS EDUCATIONAL PLATFORM: GOOGLE SUITE FOR EDUCATION

The school has subscribed to Google Workspace for Education (Fundamentals) (formerly Google Apps for Education) which gives us a controlled domain cfschool.org.uk with free access for all registered school users to a range of digital applications and storage facilities. These include:

- Email (Gmail)
- Storage (Google Drive)
- Document production (Google Docs, Google Sheets, Google Slides)
- Calendar (event and task management)
- Websites (Google Sites)
- Classroom (digital learning management tool)
- Video conferencing
- Social media (Google Hangouts)

This suite of applications has enormous benefits for staff and students provided sensible precautions are taken to keep all users safe.

3.2.1 Benefits for staff and administrators

3.2.1.1 **Googlemail** is a useful communication medium for staff, enabling them to communicate with colleagues quickly, effectively and securely.

3.2.1.2 Staff can also collaborate on documents using the **Google Docs and Google Drive** share facility. Documents can be stored within Google Workspace for Education and can be securely accessed from any computer with internet access, so staff can access documents produced at home in school and vice versa.

3.2.1.3. With many staff working part-time and with the requirement to self-isolate in the event of illness, **Google Workspace for Education** can be used to hold online staff or individual meetings enabling all staff to view and comment on issues.

3.2.2 Benefits for pupils and parents

3.2.2.1 The use of Google Workspace for Education can bring significant educational benefits for students and their parents, and facilitate partnership between school and home. This has been particularly important during prolonged periods of school closure due to mandated lockdowns or when pupils have been unable to attend school in person due to ill health or self-isolation.

Google Drive enables students to securely store documents that they have produced at home and access them quickly and easily in school and vice versa, eliminating the need for insecure memory sticks or the use of their personal email account to send or share documents to school from home and vice versa. Where appropriate, students can be given access to the *share documents* facility, so that teams of students can collaborate on a project. Staff can comment on documents that are shared with them by students, enabling students to get personal timely feedback on their work.

Google Mail within Google Workspace for Education is being used to facilitate communication between school, parents and pupils. Pupils with Google Mail accounts are able to use these to communicate with each other and with staff about school-related matters. When staff email pupils, they must always copy in the safeguarding team, using sgteam@cfschool.org.uk. Emails are increasingly used to communicate school information quickly with individual parents or to send information to groups of parents. (See section 4.14 for the protocols and procedures for sending emails to parents from staff.) All parents are able to email the school using the main school email address (info@cfschool.org.uk).

Google **Classroom** is used by staff to post school-based and home-learning materials, homework and other information for pupils. Teachers can also set assignments with relevant resource material, offer interactive support to students while working on their assignment, collect student work in and give class or individual feedback on the work done. It also enables pupils to collaborate and support one another in the completion of tasks.

Google Hangouts may be used by pupils to communicate with each other. The school actively monitors pupil accounts and if pupils are engaging in Hangout conversations that are in breach of the acceptable use agreement, their access to Hangouts may be restricted for a period of time or indefinitely. Sometimes, whole groups or cohorts may be denied access until there is evidence of sufficient understanding of what is appropriate behaviour.

Google Sites can be used by staff or pupils to create a webpage to be used internally for educational purposes. Staff or pupils who want to set up a topic webpage using the school Google domain address (cfschool.org.uk) must submit their proposal and draft website for approval by the Head of School, who will also decide who is allowed to post to the topic website, controlling access through passwords.

3.2.3 Restricted pupil access to additional Google services

With effect from 1st September 2021, all users of Google Workspace for Education default to under 18 (except Organisational Units with teachers and staff that have already indicated as 18 and older) via the age-based access setting in the Admin Console. This means that users that are under 18 will have **restricted access to additional Google services** and will no longer be able to access services without on/off controls. The school will turn applications off if monitoring indicates that they are being misused.

Additionally, for users who have YouTube turned off as a service, these users will no longer be able to access YouTube.com or YouTube apps with their Google Workspace for Education account. When locked onto the school network, pupils are able to access YouTube if they are monitored according to our monitoring protocols. This enables us to avoid the complete lock-down of access to YouTube and its educational benefits, whilst ensuring safe access by pupils and teachers to useful material.

3.2.4 Parent Access to Google Workspace for Education

Parents are given their young person's Google account login details, so they are able to find out for themselves about homework or other resources. In Google

Classroom, there is a facility for parents to be invited to receive regular updates about their child's assignment record: work that has been marked and returned, work that was handed in late and work that is missing.

3.2.5 Google Workspace for Education, data protection and data security

3.2.5.1 Google Workspace for Education complies with **GDPR regulations**. We are confident that the school is able to administer the service in compliance with current UK legislation and guidelines for schools. Google's security systems have been tested to a standard of rigour that would be impossible for us as an individual school to replicate. We are therefore satisfied that staff and student data stored on Google Drive is very secure.

3.2.5.2 Google Workspace for Education uses an encrypted HTTPS connection when staff read or send emails or access Google Workspace for Education applications. Gmail to Gmail correspondence and attached data is **encrypted** in transit between servers. All files uploaded to Google Drive are encrypted, not only from a school or personal device to Google and in transit between Google data centres, but also at rest on Google servers.

This means that staff can use their school Google Workspace for Education account to send and receive messages/documents with confidence whether they are logging in from a device (computer, phone or tablet) inside or outside of school, even if they are using public wi-fi.

However, encryption cannot be guaranteed at the recipient's end if staff send emails or other documents to people with other email providers, so extra caution should be exercised.

3.2.5.3 Even though Gmail to Gmail correspondence is encrypted, this cannot prevent security breaches if the email is sent to the wrong address. Staff must take extra care to **send emails to the right recipients**, especially when replying to group emails. Staff should not select 'reply to all' unless they are sure that all need to be included in the reply. When using an auto-complete function, staff must make sure they choose the right address or recipient before they click send.

3.2.5.4 Recipients who are carbon copied (cc) into an email can see one another's email addresses, so staff should **always use blind carbon copy (bcc)** unless they are certain that the email addresses should be revealed to all recipients. They should be careful when replying to an email to which they have been blind copied in: the other recipients will now know that they were on the mailing list.

3.2.5.5 Staff email signatures in the footer of their emails should include a link to a statement relating to the 'email terms' under which their communication is sent and received. This informs the recipient that if they receive an email that is not intended for them, they should contact the sender as soon as possible and that dissemination, distribution, copying or use of the email or its content is prohibited and may constitute a breach of civil and criminal law.

3.2.5.6 Staff should always use Google Workspace for Education's **secure cloud storage** (Google Drive) to **store school-related personal information.** Staff should not use memory sticks to store any data or documents containing personal information relating to the school, its pupils, staff, parents or third parties relating to school. Staff should consider whether important files that they may need to access urgently are backed up to an appropriate drive on the school server (not in the Downloads folder of their school network account), as a problem with the school's internet connection could prevent immediate access to documents stored on Google servers.

3.2.5.7 Our contract with Google makes it clear that **Christian Fellowship School owns the data** that we store within the school's Google Workspace for Education domain. The management tools and dashboards provided by Google make it easy for our Google Workspace for Education administrator to keep track of our usage of Google services and of our data. Google only keeps our data as long as we require them to. If we decide to no longer use Google, we can easily take our data away with us.

3.2.5.8 There are **no adverts** in Google Workspace for Education services and pupils do not see adverts when they use Google Search as long as they are signed into their school Google accounts.

3.2.5.9 **Spam blocking and phishing/virus protection** are part of the service provided by Google and complement the protection provided by the school's very secure firewall.

3.2.5.10 The school's **data retention policy** for Google accounts and Google Mail means that accounts will not be retained longer than is necessary - which for students and staff should normally be one year after they leave. The year-long retention period enables staff and students to access and store elsewhere documents that they may still require, such as student Record of Achievement statements and staff teaching material. Staff and pupils (and parents) are advised in the Acceptable Use Agreement that their school Google account will be deleted one year after they leave. The default retention period for Google

Mail is seven years, which will be reduced by the school to three years for student email but retained at seven years for staff email.

3.2.6 School Google account procedures

The following procedures are designed to minimise risks to children and staff using Google Workspace for Education.

3.2.6.1 All pupils in Y4 and above are provided with a school Google Workspace for Education account. All staff are required to register for a school network and Google Workspace for Education account which should be used for all school-related services and email communications. The school Google Workspace for Education accounts are managed by the administrators for cfschool.org.uk (currently the Head Teacher and Principal).

3.2.6.2 The **username** for school Google accounts will usually be the same as the username for access to the school network, but with a domain extension: @cfschool.org.uk. Users are issued a temporary **password** which they need to change when they first log-in to their account. The system administrators and Heads of Schools have access to the pupils' login details and can view activity on any pupil's account. The pupil's passwords cannot be changed without support from the administrators.

3.2.6.3 The school's domain administrators can permit or exclude access to different elements of the Google Workspace for Education applications. The administrators have created a number of **Organisational Units within Google Workspace for Education** for differing student and staff accounts. The Organisational Units make it possible to control which Google Workspace for Education applications are enabled for the users. The Senior LeadershipTeam will assess the risks of different year groups and users having access to various Google Workspace for Education applications. As and when it is decided that it is appropriate for a year group or individual to have access to specific Google Workspace for Education applications, they are transferred to the appropriate Organisation Unit.

3.2.6.4 Parents will be advised when their child is about to be issued with a school Google Workspace for Education account and will be asked to **give permission** for their child to use the services. They will be given their child's Google Workspace for Education account username and password, together with guidance and advice about how to monitor their child's activities on their school Google Workspace for Education account.

3.2.6.5 All users must agree to the relevant **CFS Acceptable Use Agreement** document: for Staff & Volunteers or for Pupils.

A copy of the **pupil AUA** document is made available to parents before their child is given an account and is reissued annually for review and signature. The pupil AUA makes it clear that a school Google Workspace for Education account is provided to pupils to enhance their educational experience and should only be used to communicate with other CFS users and school-related third parties for purposes that have been approved by the school. The AUA also makes it clear that school accounts are not private and activity on the account is monitored by the administrator and Heads of School.

The **Staff & Volunteer AUA** makes it clear that school Google Workspace for Education email accounts are not private and the school Google Workspace for Education administrators can monitor activity on the account and view contents. This is an essential safeguarding measure to protect both students and staff.

3.3 Use of personal devices for school-related purposes

3.3.1 It is recognised that many staff will need to use their own devices (desktops, laptops, tablets, smartphones) for school-related work, as the school is not able to provide dedicated school devices for all staff.

3.3.2 If a member of staff uses **a personal device** (home computer/laptop/ tablet/ smartphone) to access school-related documents containing personal data about pupils, parents or staff (including emails), they MUST ensure that their device or their login on the device is **securely password protected** so that no other user of the device can view this type of school data by opening the device. This means that family members should not know the password for a device or user accounts on a device if that would allow them access to school personal data.

3.3.3 Staff are advised to create **separate log-ons** to home computers/laptops/tablets and to ensure that there is a secure password/code/pattern on any smartphone if the device gives unrestricted access to the member of staff's school Google Workspace for Education account applications and data. If the password/code/ pattern is easy to copy, staff may need to set up their school Google Workspace for Education account so that it always requires a password before it can be accessed from their device(s).

3.3.4 Staff must ensure that school-related documents containing personal data about pupils, parents or staff, are **not stored on a personal device**. This means that if a home computer/laptop/smartphone is being used to create a document in Word, PowerPoint, Excel, etc, it should immediately be uploaded to the member

of staff's school Google Drive and then fully deleted from their personal device. This is necessary to ensure that we are complying with the General Data Protection Regulations. Staff can still use their personal device to store other school-related materials, such as lesson resources.

3.3.5 Staff should not use their own device(s) to take photos or video footage of children where their faces or other distinguishing features can be identified. The school has dedicated mobile phones and tablets that can be used to take photographs of pupils in lessons, at school events or on trips. The school equipment stores photos on school managed Apple and Google Photos cloud storage. Individual staff are provided with access to the Google Photos cloud storage as required.

3.3.6 If an external organisation or individual takes official authorised photographs or video footage of CFS pupils on their personal devices, they should be asked to sign a form confirming that once the material has been sent to the school it will be / has been deleted from their devices. This is for their protection as well as for the safeguarding of children.

3.3.7 Pupils are not allowed to bring in smart watches or other devices that can take and store images without the express permission of the Head of School. Sanctions for infringement of this policy will be similar to that for mobile phones.

4. Communications including social media

4.1 STAFF emailing and messaging on Google platform and social media

4.1.1 Staff should **not use a personal email account** for any school-related services and email communications. This includes sending emails about school matters to colleagues. Staff should exercise due diligence when sending emails containing sensitive or personal data, which should always be sent through Google Workspace for Education's encrypted service.

4.1.2 Staff who do not have **exclusive use of the device** on which they send and receive school emails (eg a family laptop) should ensure that they do not save their Google Workspace for Education account password on that device.

4.1.3 When emailing colleagues in the school community, staff should have regard to the **timing of their communications** in order to support staff welfare. There will sometimes be urgent matters that may need attention in the evening or weekend but generally staff should consider using the Gmail 'Schedule' facility to schedule their communications to arrive during or just before the working day. If a matter is not urgent, staff should consider whether the matter might be better dealt with through a brief chat in the next couple of days to avoid lengthy email trails. Staff should consider indicating the urgency or otherwise of a reply so that colleagues do not feel pressure to respond more promptly than is really necessary: eg - mark an urgent email with 'URGENT' or indicate in the body of the letter that you don't need an immediate response.

4.1.4 When emailing colleagues within the school community and professional contacts outside the school community, staff should adopt an appropriate **professional and courteous tone**, bearing in mind that the way we communicate will reflect both on ourselves and on the school.

4.1.5 For all but minor routine communications, staff wishing to **contact parents by email** should forward the email to their Head of School for checking and approval and to the Assistant Head (Operations & Communications) who has SLT responsibility for parent liaison. As a general rule, staff should not directly email parents without the agreement of the Head of School.

Once the content has been approved by the Head of School and Assistant Head (Operations and Communications), the email should normally be forwarded to the office to email out to the parent(s) unless the Head of School agrees that the subject/form teacher should send the email directly or it should be sent from the Head of School. Heads of School should send a copy of any email they send to info@cfschool.org.uk. The office holds up-to-date lists of parent email

addresses and these are also available in a shareable Google document for other senior staff.

Group emails should always be forwarded to the Assistant Head (Operations and Communications) so that they can be sent by Mailchimp.

Staff may ask class reps to send simple, everyday messages, such as 'Remember to bring wellies tomorrow' via a parents' WhatsApp group. Wholeschool messages, such as 'Last chance to buy tickets for school production' can be sent via the whole school Parents' WhatsApp group (co-ordinator, Kate Whiting).

Staff may sometimes email a parent directly if the information is brief and factual, although they should always copy in their Head of School and info@cfschool.org.uk.

Routine emails which have been agreed in principle in advance may also sometimes be sent directly to a parent or a small group of parents, with a copy of the email sent to the Head/Head of School or SENDCo and to the Assistant Head (Operations and Communications).

This procedure is to protect staff and ensure clear lines of communication within the school and with parents.

4.1.5 Staff may use their school Google Workspace for Education email account to **communicate with pupils,** but staff should ensure that they carbon copy sgteam@cfschool.org.uk. This account is accessible by the school's safeguarding team who are able to monitor and view all correspondence between pupils and staff.

4.1.6. Staff are able to **comment on any document** shared by a pupil but should be aware that comments can be viewed and monitored in the same way as emails by the Google Workspace for Education administrators and the Heads of School.

4.1.7 As with all the other Google Workspace for Education apps, communication between staff and pupils and between pupils within **Google Classroom** is not private and is subject to monitoring by the Google Workspace for Education administrators and by Heads of School.

4.1.8 Staff are advised that all communications using **personal social media accounts,** even on matters that are unrelated to school, are visible to a wide audience, so they should have due regard for their own professional and personal reputation, as well as that of the school.

4.1.9 Personal access to and **use of social media in school** should be kept to a minimum so as not to interfere with fulfilling school duties. .

4.1.10 Staff should not normally take or receive **personal calls on their mobile phone** during times when they are in contact with pupils. Staff may sometimes need to contact another member of staff or another third party on school business. Where possible and appropriate, staff should try to avoid times when children are present, especially during lessons. There may be exceptional circumstances when a member of staff may need to take a personal call during a lesson (for example, a family member may need to have immediate contact for a specific reason). Permission should be sought from the Head Teacher who will sympathetically consider the circumstances of each request. If permission is granted, staff members should, where possible, put the phone on vibrate mode only and use discreet means of responding to an incoming call - eg asking a TA to oversee the class for a couple of minutes and going outside the door to answer or return the call in the corridor.

4.2 Parents' digital communication on school-related matters

4.2.1 All parents are able to email the school using the main school email address: info@cfschool.org.uk. (Parents and staff are advised that office@cfschool.org.uk should not be used as this is not monitored on a daily basis.) Parents should normally only use info@cfschool.org.uk or the Head of School's email addresses and should be discouraged from communicating directly by email with subject/form teachers or other staff. If a member of staff receives an email from a parent to their individual school email address, the email should be forwarded to the Head of School and a conversation held before any reply is made.

4.2.2 The **whole school parents' WhatsApp group** is managed by a parent volunteer (currently Kate Whiting) who liaises with the Assistant Head (Ops and Comms) about content to be posted by the school. Staff wanting to post a message on the whole school parents' WhatsApp should forward this to the Assistant Head (Ops and Comms). The parent volunteer will also monitor the WhatsApp group to ensure that messages are in line with the school's expectations for content and tone of communication on CFS managed WhatsApp groups. Parents are asked to adhere to the guidance on our school website: CFS WhatsApp guidelines.pdf

4.2.3 **Class-based parents' WhatsApp groups** are used to facilitate communications with and between parents of children in a specific class. Staff wanting to get an 'everyday' message out to a class group - such as, 'Thank you to all parents who

sent in food for our culture day yesterday - it was much appreciated." may ask the class rep to post the message on the class parents' WhatsApp group. More significant messages that touch on policy, class dynamics, class concerns, etc, should be sent via email rather than the WhatsApp group, following guidelines for sending emails as outlined above. The class rep should monitor the content and tone of the class WhatsApp group and discuss any concerns with the Assistant Head (Ops and Comms).

4.2.4 Given the community nature of the school, some parents will legitimately have access to the personal mobile or landline numbers of members of staff. To protect staff from being called by parents about school-related matters during evenings and weekends, parents are requested to put school-related concerns or information about their child in writing by email or make a phone call via the school office during school hours. Parents who are friends/relatives of members of staff are also asked not to share the personal numbers of members of staff with other parents for contact outside of school hours.

4.3 Pupils' use of digital devices and social media

4.3.1 **Mobile phone**s should not be brought to school unless the parent has signed an agreement authorising their child to bring a phone to school for safety reasons. Phones that are authorised to be in school must be handed in to the office at the start of the day. Phones should be collected at the end of the school day. They should **only be used off the school premises** (which includes the grounds). If a student needs to contact their parent(s) urgently, the school office should be asked to ring on their behalf, although if the office staff are busy students may ask the member of staff on duty if they have permission to use their own mobile phone to contact a parent about any change of plan.

4.3.2 Students should not use a mobile phone on the school premises without permission. This is to avoid the risks of harm (including peer-on-peer abuse) through unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). Any phone discovered on school premises without authorisation or being used without permission, is likely to be **confiscated**. Its return to the student will be subject to the outcome of an interview with the student's parent(s). Pupils will be regularly reminded to hand in their phones, and will be informed in advance if a spot-check of bags/coats is imminent.

4.3.3 If a phone is permitted on a school trip, parents are asked to ensure that any music or images stored on the phone are in keeping with the school's Christian ethos. If a pupil is found using their mobile phone to access or share **inappropriate music or images**, the member of staff in charge of the trip has the

authority to confiscate the phone. Its return to the pupil will be subject to the outcome of an interview with the pupil's parent(s). This section should be incorporated into any school trip letter to remind parents of their responsibilities.

4.3.4 **No images or video footage** taken by a pupil at school, on a school trip or during a school event may be posted **on any social media platform** without the school's explicit authorisation.