CENTRAL FOUNDATION BOYS' SCHOOL

ONLINE SAFETY POLICY 2021/22

Table of Contents

Introduction

Central Foundation Boys' School believes that the use of information and communication technologies in schools brings great benefits. Recognising the online safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic devices and communications.

Aims

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

Key Responsibilities:

Safeguarding Lead: A Chawluk – Assistant Head Teacher

OSL (OSL) – L Stevens – Assistant Head Teacher

IT technical support – Joskos: Managed Service Provider

Technical Providers

Internet Service Provider (ISP) – LGfL

Anti-virus provider – Sophos

Email Provider

- Staff: iAMCloud (Office 365)
- Students: Google Apps for Education, iAMCloud (Office 365)

Logging a safeguarding concern

All staff at Central Foundation Boys' School are trained in using Impero Edaware when logging a safeguarding concern. This extends to safeguarding our students when they are online. Staff will log any online safeguarding concerns they may have about a student on Impero Edaware and the concern will be responded to in a timely manner by the relevant party

Why does a school need an online safety policy?

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

Schools and other settings must decide on the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff

about responsible use. Schools must be aware that children and staff cannot be completely prevented from being exposed to risks both on and offline.

Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. Breaches of an online safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider school community. It is crucial that all settings are aware of the offline consequences that online actions can have.

Schools must be aware of their legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Headteacher and the Governing Body. The online safety policy is essential in setting out how the school plans to develop and establish its online safety approach and to identify core principles which all members of the school community need to be aware of and understand

The breadth of issues classified within online safety is considerable, but can be categorised into four 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; for example: peer to 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 bullying; and
- commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Teaching and Learning

Why is Internet use important?

Internet use is part of the statutory curriculum and is a necessary tool for learning.

The Internet is a part of everyday life for education, business and social interaction.

The School has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in the School is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

Provides access to worldwide educational resources including museums and art galleries;

Encourages inclusion in the National Education Network which connects all UK schools;

Allows educational and cultural exchanges between pupils worldwide;

Provides access to experts in many fields for pupils and staff;

Helps professional development for staff through access to national developments, educational materials and effective curriculum practice;

Helps collaboration across networks of schools, support services and professional associations; Provides improved access to technical support including remote management of networks and automatic system updates;

Allows access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Internet access will be designed to enhance and extend education.

Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught and then advised to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content.

For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Pupils will use age-appropriate tools to research Internet content. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole school requirement across the curriculum.

The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

- It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.
- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.

Security

The IT managed service provider will ensure

- The server operating system must be secured and kept up to date
- The server will be backed up regularly
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.

- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The School's IT Managed Services will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.
- The Headteacher is a formal representative of the school in the administration of the services used.
- The ICT Co-coordinator is named as an approved nominated contact for the school IT service accounts, as is the Network Manager. Other staff may be nominated to administer an account, with the approval of the ICT Co-coordinator or Head teacher.
- The nominated contacts are authorized to create new accounts for the services they are representative for and adjust the settings of the system such as Internet filtering.
- The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the data protection policy
- The school email service providers include the filtering of all inbound and outbound email. Email is scanned for unwanted 'spam' emails, viruses and inappropriate language.
- The school's ISP subscription includes a sophisticated Internet filtering service which can be tailored to a school's particular preferences.
- Remote access to individual computers connected to the school's network through the schools ISP is available. A rigorous approach to the management of remote access is applied in order to safeguard pupils, teachers, personal data and valuable IT systems.
- The school will ensure that there is virus protection for every computer and server within the school.
- Neither staff nor students are allowed to download, process or send any inappropriate contents on their computers and through their email or any software or files that could overload the system or introduce viruses. Please refer to the section on *Staff, Governors and Visitors Code of Conduct*
- ICT equipment must be stored securely and ICT rooms must be locked when not in use. Staff are required to log off when they are leaving the terminal unattended or when leaving their classroom or office to prevent unauthorised users accessing the system in their absence.
- Unsupervised access by pupils to ICT rooms is not allowed.

Resources

All software used in school must be licensed and this is the responsibility of the network service provider. Only the network manager can load software on to school equipment.

The whole school ICT budget is used to purchase and maintain general, whole school ICT equipment and software. Subject specific software and equipment should be budgeted for and paid for from departmental funds unless otherwise agreed by a member of the senior leadership team. The suitability and compatibility of ICT equipment and software should be checked with the network manager before it is ordered.

Damage to Equipment

Pupils who damage equipment may be banned from using ICT equipment for a period of time. Parents/carers may be asked to pay the cost of any repairs.

Out-of-Lesson Access

When open, the LRC computer suite is available to all pupils before school and after school. Staff may also use ICT rooms for supervised, out-of-hours sessions with pupils or homework clubs.

Staff Training

ICT training sessions for staff can be arranged where a need is identified by the senior leadership team. Online safety training will take part each year as part of the safeguarding training for all staff.

If individuals require training, they can request this through the standard training request procedures.

Use of computer rooms

As with all classroom's computer rooms are to be kept tidy by the individual in charge of that room for the session and by the member of staff assigned to management of the room.

How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created.

The implications of email use for pupils need to be thought through and appropriate safety measures put in place. Unregulated email can provide routes to pupils that bypass the traditional school boundaries.

A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible.

In the school context, email should not be considered private and most schools and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations.

When using external providers to provide students with email systems, close attention will be paid to the sites terms and conditions as some providers have restrictions of use and age limits for their services. Additionally:

- Spam, publishing and virus attachments can make email dangerous
- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.

Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.

Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

Access in school to external personal email accounts may be blocked.

Excessive social email use can interfere with learning and will be restricted.

Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

The forwarding of chain messages is not permitted.

Can pupils' photographs/videos of students be published?

When joining the school parents are required to sign a Publicity Consent Form.

This will allow the use of student photographs in appropriate marketing materials e.g. school website Pupils in photographs should, of course, be appropriately clothed.

Images or videos that include pupils will be selected carefully.

Written permission from parents or carers will be obtained through the publicity consent form before images/videos of pupils are electronically published.

Publicity Consent Forms will be kept by the School.

How will social networking, social media and personal publishing be managed?

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control.

For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

The school will use filters to limit access to social media and social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.

Staff will obtain documented consent i.e. email, from the Senior Leadership Team before using Social Media tools in a school setting.

If a request is sent through to the School's IT Managed Services then this will be forwarded to the member of the Senior Leadership Team overseeing ICT.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.

Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Newsgroups will be blocked unless a specific use is approved.

Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

How will filtering be managed?

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles will be appropriate for all members of the School community.

Older 6th form pupils, as part of a supervised project, might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality.

Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available.

If a member of staff wishes to access a site that is blocked they are required to email the School's IT Managed Services who can review the suitability of the site, discuss the suitability with the Senior Leadership team and then provide access if deemed suitable.

If staff or pupils discover unsuitable sites, the URL will be reported to the School's IT Managed Services and the member of the Senior Leadership Team overseeing ICT who will

then escalate the concern as appropriate. The School filtering system will block sites centrally, this is carried out by LGFL.

If the IT Support team or a member of staff is aware of a student accessing inappropriate content then this should be raised with DoL to consider any further action under the school behaviour policy. They should also consult the designated safeguarding lead if there is a concern around safeguarding.

The IT support team can provide logs of internet access and other IT usage for any student to the relevant DoI or SLT.

How should personal data be protected?

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

Please refer to the schools *Data protection policy*

Policy Decisions

Accessing suitable material

The School will ensure appropriate filters and appropriate monitoring systems are in place and will take all reasonable precautions to ensure that users access only appropriate material.

However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The School cannot accept liability for the material accessed, or any consequences resulting from Internet use.

How will the school respond to any incidents of concern?

The reporting of concerns (such as breaches of filtering, cyberbullying, illegal content etc) will go through the respective Director of Learning (DOL) for the students concerned.

The Designated Safeguarding Lead will be informed of any online incidents involving Child Protection concerns, which will then be escalated appropriately.

The School will manage online safety incidents in accordance with the School discipline/ behaviour policy where appropriate. The School will inform parents/carers of any incidents of concerns as and when required.

After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required.

Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school may escalate the concern to the Police and any other relevant agencies.

How will online safety complaints be handled?

Parents, teachers and pupils should know how to use the School's complaints procedure.

The facts of the incident or concern will need to be established and evidence should be gathered where possible and appropriate. Online safety incidents may have an impact on pupils, staff and the wider School community both on and off site and can have civil, legal and disciplinary consequences.

Complaints about online safety will be dealt with under the School's complaints procedure.

Any complaint about staff misuse will be referred to the Headteacher or OSL.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".

Cyberbullying (along with all other forms of bullying) of any member of the School community will not be tolerated. Full details are set out in the School's policy on anti-bullying and behaviour.

All staff should be aware that children can abuse other children (often referred to as peer on peer abuse).

All staff should be clear as to the school's policies and procedures with regards to bullying and peer on peer abuse.

In an online setting this is most likely to include, but may not be limited to:

- bullying (including cyberbullying);
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse;
- up skirting - which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm that may include sharing with others. Including online through mediums such as a text or instant messaging, or through printing physical copies
- sexting – sending sexually explicit messages or images (also known as youth produced sexual imagery);
- and initiation type rituals.

There are clear procedures in place to support anyone in the school community affected by bullying. All incidents of cyberbullying reported to the school will be recorded under this policy.

- The school will take steps to identify the bully, where possible. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at the school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the school's anti-bullying behaviour policy.
    - Parent/carers of pupils will be informed.

- The police may be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

- Mobile phones and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even children in early years settings may own and use personal devices to get online regularly.
- Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.
- However, mobile phones can present a number of problems when not used appropriately:
    - They are valuable items which may be stolen or damaged; Their use can render pupils or staff subject to cyberbullying; Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering.
    - They can undermine classroom discipline as they can be used on "silent" mode;
    - Mobile phones with integrated cameras could lead to Child Protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.
- The use of mobile phones and other personal devices by students in the School is prohibited.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the School discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the School behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal School time unless as part of an approved and directed curriculum-based activity with consent from a member of the Senior Leadership Team.
- Student Mobile phones and personal devices should otherwise be switched off at all times.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items, Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual. Mobile phones and personal devices

are not permitted to be used in certain areas within the School site such as changing rooms and toilets.

Use of Personal Devices

Pupils Use of Personal Devices

- If a pupil breaches the School policy then the phone or device will be confiscated and will be held in a secure place in the School office. Mobile phones and devices will be released to parents/carers in accordance with the School policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his/her parents/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 reception.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are advised not to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- If there is a necessity for a member of staff to use their own personal device as a point of contact they should ensure that they use the "call withheld" feature.
- Staff need to be aware that "call withheld" does not work when texting and so should not text students from their personal devices
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Home Learning

Home Learning Tools

- For the aims of home learning please refer to the *Home learning policy*
- The school will provide an extension to the school curriculum through approved online apps
- A list of approved tools can be found on the school website and will updated yearly.
- Communication of any other tools to be used by students may be sent via SMHW
- The school defines an online app as a computer programs that can run on a mobile phone, smartphone or tablet or a web browser through the internet
- Where an app requires a student to register, with a login, a risk assessment will be carried out to ensure the app is age appropriate, GDPR compliant and meets safeguarding requirements
- The school will review the safety of such apps yearly and may decide to cease using an app if there are concerns about usage or pupil safety
- Online apps should not be used with pupils without approval from SLT

Live Streamed Sessions

- There may be instances where the school will offer sessions or explanations via a stream using video conferencing software
- If a member of staff is to conduct a Interactive video session with students, they should make themselves familiar with this and all linked policies.
- Communication with students may take in the format of chat or email using an approved school application
- All communication in sessions are to follow the same rules and procedures as a normal lesson, therefore any misbehaviour through virtual communication will be dealt with under the school behaviour policy
- Staff and students must be aware of their professionalism required for a session and at no point must anyone involved carry out an act that may bring the school in disrepute.

Live Interactive Sessions

- There may be instances where the school will offer live interactive sessions via video conferencing software
- If a member of staff is to conduct an Interactive video session with students, they should make themselves familiar with this and all linked policies.
- The member of staff concerned must follow school procedures for interactive video sessions and raise any concerns that may occur during the sessions through normal lines of communication
- If there are any safeguarding concerns during a session, then the session should be stopped, and the concerns raised immediately with the Director learning for that year group and the safeguarding lead
- All live interactive sessions are to follow the same rules and procedures as a normal lesson, therefore any misbehaviour within a session will fall under the school behaviour policy
- Full names should be used when joining the session as an identifier, if a student joins anonymously they should not be admitted to the session
- Any students misbehaving during the session can be removed from the session
- Staff and students must be aware of their professionalism required for a session and at no point must anyone involved carry out an act that may bring the school in disrepute.
- It is advised that One to One sessions, include two members of staff.
- If this is not possible then the session should be recorded in the school cloud and kept on the school system for a minimum of 4 weeks
- Staff should check with the IT team for support with this if required.
- Live interactive sessions are not to be conducted in any online app other than Microsoft Teams through a member of staffs school email address
- The session may be recorded for monitoring purposes, staff should outline this at the start of a session.
- No Live interactive sessions will take place without approval of the head teacher
- The head teacher may wish to delegate this responsibility to another member of SLT

Pre-Recorded Video Guidance

- There may be times where a member of staff wishes to offer recorded guidance to students, e.g. sharing a link to a self-created video through SMHW
- This type of support is at the discretion of the member of staff concerned and there is no requirement to offer this extra support.
- Staff should ensure the area of the screen being recorded contains only content suitable for students, as they would in a school setting when displaying a screen to students.
- Comments should be disabled if uploading videos to YouTube, or other online video services
- It is advised that videos be set so they are only accessible via a link and cannot be searched for in a web browser. This can be achieved through most online video services e.g. YouTube
- Any inappropriate comments or use of imagery from videos from members of the school community will be treated as cyber bullying.

Key Responsibilities and Responsible Use

All users are required to adhere to this policy.

- This section further expands on specific responsibilities and codes of conduct for individuals who use the school online systems
- Students users who misuse ICT facilities or online applications related to school will be referred to their Director of Learning and dealt within under the behavior policy.
- Other users who misuse ICT facilities or online applications related to school will be referred to the Senior Leadership team and HR.

Pupils Acceptable Code of Conduct

- I will treat myself and others with respect at all times; when I am online or using any device, I will treat everyone as if I were talking to them face to face.
- Whenever I use a device, the internet or any apps, sites and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
- I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
- It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.

- If I see anything that shows people hurting themselves or encouraging others to do so, I will report it on the app, site or game and tell a trusted adult straight away.
- I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
- I will only use the school's internet, systems, devices and logins for school-related activities for activities that are appropriate to what I am doing at that time (e.g. at school I don't play games unless I am allowed to, e.g. during lunch.
- Whenever I use the internet or devices in school **OR use school devices at home OR log in on home devices at home**, I may be monitored or filtered; the same behaviour rules always apply.
- I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
- I will not carry out any form of cybercrime
- I will not try to bypass school or other network security in any way or access any hacking files or tools.
- I will not carry out a Denial of Service (Dos or DDoS) attacks or 'booting' where a network/website causing the network to become overwhelmed with internet traffic and becomes unavailable
- I will not supply or obtaining malicious software (malware) such as viruses, spyware, ransomware, botnets and Remote Access Trojans to commit further offences
- I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
- I will use the internet, apps, sites & games responsibly; I will not use any that are inappropriate for school use or for my age, including sites which encourage hate or discrimination.
- I understand that any information I see online could be biased and misleading, so I should always check sources before sharing (see fakenews.lgfl.net for support).
- I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
- I will not post, look at, up/download or share material that could be offensive, harmful or illegal. If I come across any, I will report it immediately.

- I know some sites, games and apps have age restrictions (most social media are 13+) and I should respect this. 18-rated games are not more difficult but inappropriate for young people.
- When I am at school, I will only mail people if it's relevant to my learning.
- Messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school.
- I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will not open a file, hyperlink or any other attachment.
- I will not download copyright-protected material (text, music, video etc.).
- I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
- **When learning remotely, teachers and tutors will not behave any differently** to when we are in school. If I get asked or told anything that I would find strange in school, I will tell another teacher.
- I will only use my personal devices (mobiles, smartwatches etc) in a school setting if I have been given permission, and I will never take secret photos, videos or recordings of teachers or students, **including when learning remotely.**
- I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
- What I do on devices should never upset or hurt others & I shouldn't put myself or others at risk.
- If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
- It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
- I can always say no online, end a chat or block someone; if I do, it's best to talk to someone, too.
- I will raise concerns with trusted adults at school, home and elsewhere and I can also get in touch with Childline, The Mix, or The Samaritans.

Pupil Conduct During a Period of Home Learning (e.g. Home delivery due to COVID 19)

- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- To understand that the school behaviour policy, anti-bullying policy and online safety policy still applies to student's code of conduct whilst in the home learning setting and that sanctions, including exclusion, could apply for inappropriate behaviour
- To follow the normal process to report concerns as when in the school setting.
    - Students can highlight any concerns to the Director of Learning for their year group during the phone calls made, or to another member of staff via the communication feature in SMHW
    - If they or someone they know feels worried or vulnerable or has another concern when using online technology, then this should be raised with a member of staff either by the student or parent/carer
- When using email students must only communicate to members of staff via that staff members official school email addresses

Staff Key Responsibilities

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Read and follow this policy in conjunction with the school's main Safeguarding Policy
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations and procedures outlined in this policy and other related policies.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene and publishing strategies.
- Prepare and check all online source and resources before using.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Staff, Governors and Visitors Acceptable Code of Conduct

- I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
    - not sharing other's images or details without permission

    - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

- I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the member of SLT in charge of online safety (OSL)
- I understand the importance of upholding my online reputation, my professional reputation and that of the school) and I will do nothing to impair either. More guidance on this point can be found in this Online Reputation guidance for schools.
- Further details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety Policy.
- I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the member of SLT in charge of online safety (OSL) and the IT support team if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.
- I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.
- I understand and support the commitments made by pupils/students, parents and fellow staff, governors and volunteers in relation to their acceptable use and will report any infringements in line with school procedures
- I will follow the guidance in this policy, the safeguarding policy and all other related policies for reporting incident: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture.
- I understand that breach of this policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Staff, Governors and Visitors conduct during Home Learning

- **I will not behave any differently** towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- **I will not attempt to use a personal login for remote teaching** or set up any system on behalf of the school without SLT approval.
- **I will not take secret recordings or screenshots** of myself or pupils during live lessons.
- **I will conduct any video lessons in a professional environment** as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
- If anything, inappropriate happens or anything which could be construed in this way. **I will raise any issues for live lessons following the procedures surrounding behaviour or safeguarding.** This is for my protection as well as that of students.
- I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

Parents/Carers Key Responsibilities

- Consult with the school if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Some parents might be seeking extra support through online private tutoring
    - Parents and students, please be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.
    - Social networking sites can connect people with similar or even very different interests.

- Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others
- Users can be invited to view personal spaces and leave comments, over which there may be limited control.
- When keeping yourself safe on the internet remember never to give out personal details of any kind which may identify you and/or your location.
- Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc
- Parents should also ensure students are aware of the risks when using online resources.

- The school will offer a yearly online safety session for parents, that all parents are invited to.

Supporting school policies:
Anti-Bullying Policy
Home Learning Policy
Behaviour Policy
Safeguarding Policy
Complaints Policy and Procedure
Data protection policy