CRESTWOOD
COMMUNITY SCHOOL

ONLINE SAFETY POLICY

Introduction
Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and effective communication and collaboration between all staff. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE) and other statutory documents. It is designed to sit alongside the School's statutory Safeguarding Policy and Behaviour Policy. Any issues and concerns with online safety must also follow the school's safeguarding and child protection procedures.

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area, as well as nationally. Although many aspects will be informed by legislation and regulations, KCSIE stresses making use of teachers' day-to-day experience on the ground. This will help ensure that the policy affects day-to-day practice. Acceptable Use Policies for different stakeholders help with this.

Internal school channels should always be followed for reporting and support, as documented in school policy documents, especially in response to incidents that should be reported in line with the School's Safeguarding Policy.

Legislation and Guidance
Legislation and guidance
This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

Aims of this Policy
This policy aims to:

- This policy applies to all members of the Crestwood Community School community (including staff, governors, volunteers, contractors, students, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.
- 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 and learning, promote attainment and progress, and prepare students 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
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns

What are the main online safety risks today?

The internet is, in general, an inspiring and positive place. It is an amazing resource which enables children and young people to connect, communicate and be creative in a number of different ways, on a range of devices. However, the internet is always changing, and being able to keep up to date with students' use of technology can be a challenge. We may sometimes feel that our students have better technical skills than we do; however, children and young people still need advice and protection when it comes to managing their lives online. Issues that our students may encounter on the internet will vary depending on their age and online activities. Potential online risks can be grouped into four categories (**The 4 Cs**).

- **Conduct:**
  Students may be at risk because of their own behaviour, for example, by sharing too much information. They need to be aware of the impact that their online activity can have on both themselves and other people, and the digital footprint that they create on the internet. It is easy to feel anonymous online and it's important that students are aware of who is able to view, and potentially share, the information that they may have posted. When using the internet, it is important to keep personal information safe and not share it with strangers. Students should know the importance of reporting inappropriate conversations, messages, images and behaviours and how this can be done.

- **Content:**
  Students may be accessing age-inappropriate or unreliable content. Some online content is not suitable for students and may be hurtful or harmful. This is true for content accessed and viewed via social networks, online games, blogs and websites. It is important for students to consider the reliability of online material and be aware that it might not be true or written with a bias. Students may need our help as they begin to assess content in this way. There can be legal consequences for using or downloading copyrighted content, without seeking the author's permission.

- **Contact:**
  Students can be contacted by bullies or people who groom or seek to abuse them. It is important for students to realise that new friends made online may not be who they say they are and that once a friend is added to an online account, they may be sharing their personal information with them. Regularly reviewing friends' lists and removing unwanted contacts is a useful step. Privacy settings online may also allow them to customise the information that each friend is able to access. If a student is, or has been, the subject of inappropriate sexual contact or approach by another person, it should be reported to the police. Students should know how to report it online via the Child Exploitation and Online Protection Centre (www.ceop.police.uk) and need to know the importance of telling a trusted adult straight away if someone is bullying them or making them feel uncomfortable, or if one of their friends is being bullied online. If a student is the victim of cyberbullying, this can also be reported online and offline.

- **Commercial:**
  Students can be unaware of hidden costs and advertising in apps, games and websites. Their privacy and enjoyment online can sometimes be affected by advertising and marketing schemes, which can also mean inadvertently spending money online, for example within applications. Students should be encouraged to keep their personal information private, learn how to block both pop ups and spam emails, turn off in-app purchasing on devices where possible, and use a family email address when filling in online forms.

The 4 Cs do not stand in isolation, however, and it is important to understand the interplay between all four. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming or images (formerly known as 'sexting').

Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare students for life after school. There is a duty to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school.

Headteacher and Senior Leadership Team: Key responsibilities

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

Designated Safeguarding Lead and Deputy DSLs: Key responsibilities

- The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." KCSiE
- Ensure "an effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." KCSiE
- Liaise with the local authority and work with other agencies in line with Working together to safeguard children". KCSiE
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others)
- Receive regular updates in online safety issues and legislation, and be aware of school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure the guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying

- Facilitate training and advice for all staff:
    - All staff must read KCSIE Part 1 and all those working with children Annex A
    - It would also be advisable for all staff to be aware of Annex C (online safety)
    - Cascade knowledge of risks and opportunities throughout the organisation

Governing Body: Key responsibilities

- Approve this policy and strategy and subsequently review its effectiveness
- Ensure an appropriate senior member of staff, from the senior leadership team, is appointed to the role of DSL with lead responsibility for safeguarding and child protection (including online safety) with the appropriate status, authority and time, funding, training, resources and support". KCSiE
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- Ensure that all staff undergo regular safeguarding and child protection training (including online safety) at induction". KCSiE
- Ensure appropriate filters and appropriate monitoring systems are in place whilst being careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". KCSiE
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school or college approach to online safety with a clear policy on the use of mobile technology." KCSiE

All Staff: Key responsibilities

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) is
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education
- 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.
- Sign and follow the staff acceptable use policy, social media policy, code of conduct
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of learning opportunities as they arise
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what students/students are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide students when engaged in learning activities involving online technology supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Check all online resources before using within the classroom
- Encourage students/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom
- Receive regular updates from DSL and have a healthy curiosity for online safety issues
- Promote online safety with targeted assemblies and tutor time activities as part of the pastoral curriculum.

- 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.

Network Manager: Key responsibilities

- As listed in the 'all staff' section, plus:
- Work closely with the DSL / DPO to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems
- Support & advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher / SLT to ensure the school website meets statutory DfE requirements

PSHE Lead: Key responsibilities

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety in accordance with the national curriculum in conjunction with the Achievement Leader for Technology
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their students' lives." KCSiE.
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that students face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE/PDL.

All Achievement Leaders: Key responsibilities

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

- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and students alike
- Work closely with the DSL/SLT and all other staff to ensure an understanding of the issues, approaches and messaging within their subject

Data Protection Officer: Key responsibilities

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents such as KCSiE.
- Be aware that GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children.
- Work with the DSL, Headteacher, SLT and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers, Contractors and External Groups: Key responsibilities

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- Maintain an awareness of current online safety issues and guidance
- 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, students or other parents/carers.

Students: Key responsibilities

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

Parents/Carers: Key responsibilities

- Read the student AUP and encourage their children to follow it
- 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, students or other parents/carers.
- Ensure their child has read, understood and agreed to the terms on the school's acceptable use policy
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? – UK Safer Internet Centre
    - Hot topics – Childnet International
    - Parent resource sheet – Childnet International

Educating students about online safety

Students will be taught about online safety as part of the curriculum:

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- By the **end of secondary school**, students will know:
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

Cyber-bullying
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Dealing with online-safety concerns and incidents
It is vital that all staff recognise that online-safety is a part of safeguarding. General concerns must be handled in the same way as any other safeguarding concern so all staff should err on the side of talking to the DSL to contribute to the overall picture or highlight what might not yet be a problem. Reporting should be done through ClassCharts.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence). School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Keeping Children Safe in Education
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation

Crestwood Community School commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact students when they come into school). Staff are encouraged to report issues swiftly to allow them to be dealt with quickly and sensitively through the school's escalation processes.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed. We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or students engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

Youth produced sexual imagery: 'Sharing of nudes and semi nudes'

Sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'. Never view, download or share the imagery yourself, or ask a child to share or download, this is illegal. Where one of the parties is over 18, this is no longer sexting but child sexual abuse

- If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to), report this to the DSL
- Do not delete the imagery or ask the young person to delete it
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers
- Do not say or do anything to blame or shame any young people involved
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies should outline codes of practice to be followed. The school DSL will decide the next steps and whether other agencies need to be involved. It is important that everyone understands that whilst sexting is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that students/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Sexual Violence and Harrassment (Update for 2022)

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

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language. It is also understood by staff that these behaviours are often perpetrated by child on child.

Misuse of school technology (devices, systems, networks, platforms)

Clear and well communicated rules and procedures are essential to govern student and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy as well as in this document.

Where students contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social Media
See the social media section later in this document for rules and expectations of behaviour for children and adults in the Crestwood Community School community. These are also governed by school Acceptable Use Policies and the school social media policy. Breaches will be dealt with in line with the school behaviour policy (for students) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the school will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

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

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

Students are not allowed to be 'friends' with, or make a friend request to, any staff or governors. Students are discouraged from 'following' staff or governor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts. Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL / Headteacher.

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

Email
Students and staff at Crestwood Community School use the school's GMail accounts for all school emails. School email addresses are fully auditable, trackable and managed by the Network Manager. This is for the mutual protection, safety and privacy of all staff, students and parents, as well as to support data protection. Email / Google Classrooms are the only means of electronic communication to be used between staff and students. Microsoft Teams may be used when working Children Services or the Police.

There should be no circumstances where staff use a private email to communicate with a student. If this happens by mistake, the DSL/Headteacher should be informed immediately. Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Students and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images or malware are likely to be blocked and not arrive at their intended destination.

Cloud Platforms
Only school-approved platforms (e.g. Google Drive) are used by students or staff to store student work.

Digital images and video
When a student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose and for how long. Whenever a photo or video is taken/made, the database of consents will be checked before using it for any purpose. Any students shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. Members of staff may occasionally use personal phones to capture photos or videos of students, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services. Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

Personal devices including mobile phones, wearable technology and bring your own device (BYOD)
Students are not to use mobile phones on the school site. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission will lead to the phone being confiscated and it being held in reception until the end of the school day. Important messages and phone calls to or from parents can be made at the school office or the Pastoral Team, which will also pass on messages from parents to students in emergencies.

Students may use their mobile phones whilst they are still on-site at the end of the school day (from 2.50pm). However, they are allowed to access the school wireless internet network for school related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.

Network / internet access on school devices
School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. There will be regular reviews and audits of the safety and security of school/academy technical systems. Servers, wireless systems and cabling must be securely located and physical access restricted.

- All users will have clearly defined access rights to school/academy technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password. It is therefore advised that the password provided is changed to a more personalised and secure one.
- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the Headteacher/DSL and kept in a secure place (e.g. school safe)
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider, Smoothwall. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" onto the school systems.

Trips / events away from school
For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with students/students and parents.

Training
All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse, Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term
-

The DSL/DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Searching and confiscation

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

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL/headteacher/other member of theSLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Appendices

- Legislation (Link)
- School Policies
    - Staff code of Conduct (Link)
    - Safeguarding Policy (Link)
    - Social Media Policy (Link)
    - Remote Learning Policy (Link)
- Acceptable use agreements:
    - Student ICT Agreement (Link)
    - Student Laptop Loan Agreement (Link)
- BYOD policy statement (Link)
- Internet Filtering and Monitoring (Link)