Online Safety Policy

THE GRANGE SCHOOL

Document Name	Online Safety Policy
Version Number	RDOSGFEB2024
Date	February 2024
Document Owner	Head of the Senior School/Chief Operating Officer
Next Review Date	February 2025
Statutory/Non Statutory	Non Statutory

Online Safety Policy

THE GRANGE SCHOOL

REVIEW DATES AND APPROVAL

This policy is reviewed by the Nominations & Compliance Committee and then approved by the Full Board of Governors (including the Chair of Governors and the Head(s)).

Last reviewed: February 2024

Next review: February 2025

Person responsible for review: Head of the Senior School/Chief Operating Officer

1. Aims and Objectives

It is the duty of The Grange School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning, but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Prevent Strategy / policy / procedures

- Staff Code of Conduct;
- Behaviour Policy
- Staff Code of Conduct;
- Data Protection Policy and Privacy Notice/s;
- School Trips Policy
- PSHE / RSE Policy;

At The Grange School we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

2. Scope

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:

- "staff" includes teaching and non-teaching staff, governors, and volunteers;
- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's [Behaviour Policy and / or Safeguarding and Child Protection Policy] as is appropriate in the circumstances.

3. Roles and responsibilities in relation to online safety

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

3.1. The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the [Online safety Coordinator, DSL and Senior Leadership Team] are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

3.3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at The Grange School This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Headteacher, Senior Leadership Team and Head of IT to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the Head of IT and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

3.4. Online Safety Coordinator

The DSL has delegated day to day responsibilities relating to online safety to the school's [Online Safety Coordinator]. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Coordinator will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

3.5. IT Services staff

The school's Head of IT and IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Senior and Junior DSL and Leadership Teams.

3.6. Teaching and support staff

All staff are required to sign and return the IT Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL and the Headteacher and Senior Leadership Teams as appropriate.

3.7. Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

3.8. Parents and carers

The Grange School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

4. Filtering and Monitoring

In general:

The Grange School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The DSL/Online Safety Coordinator will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding and/or Online Safety governor, the DSL and Online Safety coordinator will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as, but not limited to, our filtering categories and alerts stances. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact IT Services for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, IT Services will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify their Head of Department, IT Services and the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL and Head of IT immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL and Head of IT.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the head of their department / IT Services and the DSL if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to their form or classroom teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems, school devices and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact a member of IT Services staff and their teacher for assistance.

5. Education and training

5.1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the IT Acceptable Use Policy which must be signed and returned before use of technologies in school.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

5.2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL Online Safety Coordinator and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through [discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Anti Bullying / Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should

approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore aims to arrange annual discussion evenings for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6. Use of school and personal devices

WiFi is accessible to Staff and students for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored. The school also extends WiFi access on an invitation only basis to approved 3rd parties such as contractors, patrons and parents.

All and any usage of devices and/or systems and platforms may be monitored and tracked.

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use. Staff are referred to the Staff and Visitors BYOD Policy, staff code of conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. Exceptions are made two-factor authentication (2FA), where it forms an important security protection to school systems.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction section Digital images and video, along with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies. Child/staff data should never be downloaded onto a private device.

Pupils

Junior Pupils: Please also refer to Junior School rules policy.

Senior Pupils: Please refer to the Senior Mobile Phone and Electronic Devices policy.

Junior/Senior pupils who bring in mobile devices (e.g. for use during the journey to and from school), they must be handed to the Form Teacher at the start of the day and collected before leaving school at the end of the day. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies. Devices remain the responsibility of the child in case of loss or damage. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with form tutors or Head of Year to agree how the school can appropriately support such use. A member of SLT will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

Volunteers, contractors, governors should leave their phones in their pockets and turned off/silent. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g., for contractors to take photos of equipment or buildings), permission of either headteacher/COO/Head of IT/Head of Estates should be sought and this should be done in the presence of a member staff.

Parents are asked to leave their phones in their pockets and turned off/silent when they are on site. Exceptions are made in Junior School playgrounds for drop-off or collection. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document and information outlined at each event. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

7. Authorised Systems

- All digital platforms and subscriptions can only be approved by Head of IT.
- Pupils at The Grange communicate with each other and with staff using
    - Email via Microsoft Office 365 (Junior School pupils are limited to internal sending only)
    - Microsoft Teams (Policy enforced so a Staff member must be in a chat for student-to-student chat to occur to allow adequate monitoring)
    - Firefly messaging for Junior and Senior School students.
    - Seesaw messaging for Junior School younger students.
    - Other digital platforms and subscriptions as approved by Head of IT.
- Staff at this school use the email system provided by Microsoft for all school emails. They never use a personal/private email account (or messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual

protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed. As such, All digital systems, platforms and subscriptions can only be approved by Head of IT.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the Head of IT/DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

8. Online storage or learning platforms

All the principles within this policy also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

We have strict guidelines around the staff use of online storage and learning platforms, this advice is within our GDPR stances, including Data Protection Policy and our yearly editions of GDPR Practices for Staff.

9. Online Communications

Staff

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / recent alumni (i.e. pupils over the age of 18 who have left the school within the past 12 months) or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. Under no circumstances may staff contact a pupil or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system nor should pupils, parents and recent alumni / their parents / carers be added as social network 'friends' or similar.

Staff must immediately report to the DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Services.

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.

For school trips/events away from school, teachers will be issued a school trip phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number. Refer to Educational Visits Policy for more information.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work assignments / research / projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact IT Services for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the DSL.

10. Use of social media

When using social media (including all apps, sites and games that allow sharing and interaction between users) we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure (refer to policy) should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media involving pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they

arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Digital Family Agreement to help establish shared expectations and the Top Tips for Parents poster along with relevant items and support available from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

Pupils

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate].

Staff

Social media is a fast-evolving area and as such the content of this policy might not always reflect the latest technologies available. However, the following broad general principles should apply to the use of social media by staff with further explanation being available in the body of the policy below or in the separately available guidance on specific social media services.

Staff General Principles:

- The primary means of electronic communication with students should be through Firefly/Teams/Email whenever possible. If this is not suitable then other school approved mechanisms may be used such as, Instagram, Office 365, SOCs etc.
- Any accounts used for school purposes must be set up using a school email address.
- Staff should not make direct/private connections with or communicate with students via personal social media.
- For personal social media where the account is publicly accessible staff should ensure any content posted is appropriate and in line with the Grange values, especially when they are personally identifiable from the account or if they mention their status as an employee of the Grange School.
- No original images of students at all from The Grange community should be generated or uploaded on a member of staff's personal social media account. For the avoidance of doubt this does not prevent staff re-sharing material from Grange accounts.
- All student images shared via social media should be checked against GDPR and be sent out via The Grange department accounts.
- Staff are expected to use professional judgement and be mindful of the impact of their generated content upon The Grange and the wider community.
- In order to maintain professionalism, all members of staff should not give out their personal social media details to parents or students of the school.

Staff must not access social networking sites which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or staff-only areas of school.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring The Grange School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

11. Data protection

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy.

The data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

12. Safe use of digital and video images

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. More guidance is provided to staff in our GDPR policies.

Any pupils shown in public facing materials have opt-in GDPR procedures in place.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At The Grange School, no member of staff will ever use their personal phone to capture photos or videos of pupils.

Photos are stored on eStream or Photo Drives in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded at events about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Mobile Phones, Cameras or filming devices

Junior EYFS for Staff

- All members of staff lock their mobile phones away before teaching or working in our EYFS. This also means no personal cameras or filming devices are used in this setting apart from school-owned devices and those must be approved for use by the Junior School Head.

Parents/Contractors/Visitors (also including older senior students):

- Sign into site electronically and agree to the following:
- I will leave my phone in my pocket and turned off/silent. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site (including EYFS), staff or pupils/students. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of either headteacher/COO/Head of IT/Head of Estates should be sought and this should be done in the presence of a member staff.

13. Artificial Intelligence

Any usage by pupils of generative AI tools such as ChatGPT is only permitted in the circumstances outlined by their classroom teacher and subject to any conditions imposed.

In particular, personal or confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff / DSL.

14. Misuse

The Grange School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

15. Complaints

As with all issues of safety at The Grange School if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to the school's DSL in accordance with the school's Safeguarding and Child Protection Policy