



Online Safety Policy (incl. acceptable use and use of images)

Version	Date	Description	Chair of Committee	Ratified (Y/N)	Next Review Due
1	January 2024	Draft presented to Curriculum Committee	Hilary Crooks	Y	January 2026
2	June 2026	Draft presented to Curriculum Committee	Lucie Calow	Y	June 2028
3	October 2026	Draft presented to Curriculum Committee	Lucie Calow	Y	October 2028

Statement of intent

Granta School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal Framework

This policy has due regard to all relevant DfE legislation, guidance and GDPR regulations including, but not limited to, the following:

This policy operates in conjunction with the following school policies:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Positive Behaviour Support Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Use of Images Policy
- Remote & Blended learning policy
- Device agreements (see appendices)
- Safeguarding Adults at Risk Policy and Guidance

2. Roles and Responsibilities

The governing body will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the Designated Safeguarding Lead/Deputy Designated Safeguarding Lead's (DSL/DDSL's) remit covers online safety.
- Reviewing this policy on a bi-annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the Senior Leadership Team and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The headteacher will be responsible for:

- Ensuring that online safety is a running theme throughout the relevant school's policies and procedures, including in those related to the curriculum, training and safeguarding.
- Supporting the DSL and DDSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.

The Designated Safeguarding Lead and Online Safety Lead will be responsible for:

- Taking the lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with Special Educational Needs and Disabilities face online.
- Liaising with relevant members of staff on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.

Communications Officer (with support from ICT service) will be responsible for:

- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Adhering to the Pupil Device Agreement supported by a trusted adult
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.

3. Managing Online Safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors will receive regular training organised by the online safety lead
- Staff will receive regular email updates regarding online safety information and any changes to online safety guidance or legislation from the online safety lead.
- Online safety is integrated into learning throughout the curriculum

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL/DDSL, who investigates concerns with relevant staff members, and manages concerns in accordance with relevant policies depending on their nature.

Where there is a concern that illegal activity has taken place, SLT will contact the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded on CPOMS.

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-Bullying Policy.

5. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL/DDSL.

6. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL/DDSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL/DDSL without delay.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL/DDSL without delay.

7. Mental Health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL/DDSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

8. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, with the intent to scaremonger or to distress individuals who come across it.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. An online challenge becomes harmful when it could potentially put the participant at risk of harm.

Online sites that incite/encourage users to self-harm or harm to others should be reported to the police.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to SLT immediately. Further advice may be sought from ICT service or Education Safeguarding team.

9. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and ‘booting’, which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil’s use of technology and their intentions with regard to using their skill and affinity towards it, the DSL/DDSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

SLT will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The Online safety lead with support from the DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

Online safety is embedded throughout our curriculum; however, it is particularly addressed in the following subjects:

- Relationships, Sex and Health Education (RSHE) - *secondary*
- Relationships and health education - *primary*
- Personal, social, health and economic education (PSHE)
- Citizenship

- Computing

Online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The online risks pupils may face online are always considered when developing the curriculum.

The online safety lead will be involved with the development of the school's online safety curriculum working with teachers to ensure the curriculum is tailored to our wide ranging pupil cohort at Granta.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers will review external resources prior to using them, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will log the concern on CPOMS.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of Images

The collection, storage and sharing of personal data, including photographic images of children, young people & staff is governed by the UK General Data Protection regulations (UK GDPR) and the Data Protection Act 2018.

The use of images at Granta is integrated into whole school practice. Signed consent for the use of images is obtained by the pupil's parent/carer through the schools general

information form, which is kept centrally in the school office. This covers all cases where images of pupils can be used within school and by third parties. We define 'images' as any photograph or video. Consent will also be sought from those pupils who have an informed understanding and can communicate whether they would be happy with their photo being taken and shared following staff explanation of what their photo/video clip will be used for.

This consent is considered valid for the entire period that the child/young person attends Granta school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw permission in writing at any time.

Images of pupils and staff are stored on the school's computer equipment and network.

Images of pupils and staff are not permitted to be stored indefinitely on portable media.

Rights of access to these images are restricted to the staff and pupils within the confines of the school network or other online school resource. At the end of each school year the class teacher has the responsibility to retain a small number of images of each of the pupils in their class and saved in the relevant pupil file, demonstrating a particular skills or achievement and deleting all others.

The following points apply to all images of pupils:

- Where possible, general photos of classrooms or group activities rather than close up pictures of individuals should be used.
- Pupils should be in suitable dress.
- The broad range of our pupil diversity should be reflected in images used throughout the school.
- The pupil is happy to be photographed/videoed

Permission should be sought for staff images before being used and the purpose of the image explained to them.

We can divide use of images within Granta School into the following categories;

- i) Images taken by school required for school's public task e.g. learning tasks on a school display board.

These images should be removed/deleted once the CYP/staff member is no longer attending Granta or the image is no longer needed for its original purpose.

- ii) Images taken by school not required for the school's public task.

This includes images for the school website, social media and marketing purposes. If a pupil is named, avoid using the image, if the image is used, avoid naming the pupil.

Care should be taken to avoid the possibility that people outside the school could identify and then attempt to contact pupils or a member of staff directly.

iii) Parents wishing to take images at school events

The Data Protection Act does not prevent parents/carers from taking images at school events, but these must be for their own personal use. At Granta parents have to sign on arrival at an event confirmation that they agree to this. Any other use requires the consent of the parents/carers of other pupils in the image.

Staff should challenge anyone who is seen using a device that has the ability to capture images at a school event they do not recognise.

iv) Images taken by the media

Granta will inform parents/carers and staff clearly about the purpose of media photographs, so they can make an informed decision about consent. Granta School will check any official photographer's validity incl. what checks have been undertaken. Photographers will be supervised as part of our safeguarding practice.

v) Images taken by third parties

Copyright of an image including those downloaded from the internet usually rests with the person who produced it. Before using an image from a third party, schools should check that the third-party owns copyright of that image.

vi) Images taken by pupils and staff on their own devices

Pupils & staff are not permitted to take images within school or on educational visits using any personal device. Images will only be taken on school owned devices.

If pupils or staff are found to be or known to have taken images on their personal devices, this will be immediately reported to the Headteacher. The pupil will be required to delete the image/s, their personal device confiscated and parents/carers informed.

The staff member will be dealt with under the schools' disciplinary procedures.

Consent must be obtained by all parties appearing on web cams, as part of planned communication or home/blended learning. For specific information please refer to remote learning guidelines.

We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

Staff and pupils are not permitted to use personal digital equipment, such as mobile phones and cameras to record images of pupils without advance permission from the Headteacher. Pupils and staff must also have further permission from the Headteacher before any image can be uploaded for publication.

13. Use of technology in the classroom

A wide range of technology will be used during lessons, including, but not limited to, the following:

- Computers
- Laptops
- Tablets
- Interactive boards
- Intranet
- Internet
- Smart speakers
- Bluetooth
- Cameras
- Audio/Video recording

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law, seeking advice from our communications officer. Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Staff will use add free versions of site where they are available. Staff will not use open searches in the classroom when pupils are present. Staff will need to pre-search and pre-load any resources required for the lesson including video clips.

14. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the pupil agreement (see appendix)

Staff will use all smart technology and personal technology in line with the school's policies. Procedures and device agreements.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

Where there is a significant problem with the misuse of smart technology among pupils, the school will manage this in line with our Positive Behaviour Support policy.

SLT will have conversations with individuals or groups, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

Staff will seek to ensure that they are kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate consequences.

15. Use of Location tracking

This section includes expectations regarding the use of personal and organisational location-tracking technologies – including but not limited to Apple AirTags, Life360, Tile, Samsung, SmartTags and similar devices or apps – on site⁴ and during any activity involving pupils, staff or visitors. These technologies can support safety when used appropriately, but they also present risks related to privacy, safeguarding and data protection. Any use of tracking technology must comply with UK GDPR, the Data Protection Act 2018 and safeguarding best practice.

The school understands that parents may use location-tracking technologies on school transport, as many of our pupils are non-verbal, do not have their own devices to contact parents and have a long school journey.

Use of these technologies, should consider the following;

- Have a clear, legitimate safeguarding or operational purpose
- Explicit, informed consent has been obtained from the individual being tracked, or their parent/carer if under 18
- Use has been authorised by the DSL or a member of the SLT.
- Use is for the sole intention authorised
- Data collection is limited to what is necessary, stored securely and only retained if required for an agreed period.

The school does not agree with the following use:

- Placing devices on pupils, staff or visitors without their knowledge and consent.
- Using apps to monitor pupils' movements during the school day
- Any form of covert tracking
- Using tracking data to monitor personal behaviour or performance
- Sharing or exporting location data without authorisation

Staff must: report any suspected misuse of tracking devices immediately to the school Online Safety Lead or DSL, ensure any approved use is documented, store and handle any location data in line with data protection requirements.

Parents must: inform the school if their child carries a personal tracking device, ensure the device does not record or transmit data in ways that compromise the privacy of others.

Pupils must: not place tracking devices on others, use personal devices responsibly and in line with school policies.

Any concerns about unauthorised tracking will be treated as a safeguarding matter. We may; confiscate the device, inform parents/carers, refer to external agencies where appropriate.

15. Use of mobile phones (pupils & staff)

Pupils who bring a mobile phone into school should hand it in to a member of staff in the morning. Mobile phones are then stored securely in a locked box within a locked cupboard in the classroom, mobile phones are then returned to pupils at the end of the day. If a pupil refuses to abide by this rule, a senior leader is informed to request the mobile phone.

The only exceptions are if the mobile phone is used for medical or regulation purposes, which is approved by a member of the Senior Leadership Team.

Pupils are permitted to take mobile phones on residential visits, but they are kept safely and securely by a member of staff. Pupils can request to use them to make a phone call home, but for no other action.

Staff should not have mobile phones on their person during the school day. They are able to use mobile phones during break times in the staff room, or off site.

If staff members need to have their mobile phone on their person during the school day e.g. waiting for a call from a doctor, the staff member should seek prior agreement from a member of the Senior Leadership Team.

When using a school owned mobile phone, the staff member using the phone is responsible for its security. It is not to be left unattended or on display (especially in a vehicle). Staff should report the loss or theft of any school mobile phone equipment immediately.

The school remains responsible for all call costs until the phone is reported lost or stolen. Staff must read and understand the user instructions and safety points relating to the use of a school mobile phone prior to using it. School SIM cards must only be used in school provided mobile phones. Staff should not call premium rate numbers or any numbers outside of the UK, unless absolutely necessary.

Staff should understand it is illegal to use a hand-held device whilst driving. Only emergency calls may be made if it would be unsafe to stop.

16. Use of Mobile Phones as Medical Devices (pupils & staff)

At Granta we recognise that some individuals rely on mobile-linked technology to manage long term health conditions. The use of a mobile phone for medical purposes is considered a reasonable adjustment under the Equality Act 2010. Use must be safe, discreet and strictly limited to medical monitoring.

Mobile phone use for medical purposes must be formally agreed for: pupils through and Individual Health Care Plan or medical risk assessment and agreement between parents, medical professionals, Headteacher and DSL; staff through occupational health guidance, staff risk assessment and agreement from a senior leader.

A mobile phone can be used for:

- Receiving real time reading from a CGM device
- Responding to medical alerts
- Logging or checking medical data
- Communicating with parent/carer or medical professional only when medically necessary

The device:

- Must be used discreetly
- Remain on silent or vibrate mode (unless medically unsafe)
- Must not be used for calls, messaging, social media, gaming or browsing by pupils during the school day

Pupils' storage arrangements will be personalised and included in their risk assessment. Staff may keep their device on their person, but should check alerts discreetly and step out of class if needed.

Parents must provide accurate medical information, ensure devices are set up safely and securely and communicate any changes in their child's medical needs in a timely manner.

School staff should be aware which pupils/staff have authorised medical device phones and respond calmly and supportively to alerts. They should model appropriate, discreet use and report any concerns to a senior member of staff.

Medical data is confidential and staff must not access a device unless needed for immediate safety. All use must comply with GDPR and safeguarding policies

17. Educating parents/carers

The school will work in partnership with parents/carers to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement for pupils when they join Granta and as it is reviewed. They are encouraged to go through this with their child/young person to ensure their child/young person understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources
- **Granta website has relevant information on Online Safety**

18. Internet access

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately. Visitors will be required to use our guest wifi.

Granta provides pupils with supervised access to internet resources through the school's internet. Staff will preview any recommended sites before use and pupils will only be allowed to use the sites as instructed by the class teacher that have been pre-checked. Raw image searches are discouraged when working with pupils. If internet research is set for homework/home learning, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise the work. All users must observe software copyright at all times, It is illegal to copy or distribute school software or illegal software from other sources. All users must observe copyright of materials from electronic sources.

Staff must not post, personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience. Staff may use the school's name or school email address to access approved website in consultation with the senior leadership team.

Online gambling or use of personal social media whilst onsite using the school network is not allowed.

19. Filtering and monitoring online activity

The governing body will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'. At Granta we use -Netsweeper-. The governing body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The filtering and monitoring systems the school implements will be appropriate to pupils' ages and development, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The communications officer will undertake checks on the filtering and monitoring systems to ensure they are effective and appropriate. The online safety lead will check routinely ~~smoothwall~~ Netsweeper alerts and report any concerns to DSL/Headteacher.

Governing bodies and proprietors should ensure that a review of their filtering and monitoring systems effectiveness is carried out at least once every academic year. Reviews should be carried out by the SLT member responsible for filtering and monitoring, with the support of the school's designated safeguarding lead and IT support. They should include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record should be kept of these checks.
KCSE 2026

Requests regarding making changes to the filtering system will be directed to the headteacher, who will take advice before agreeing to changes. The communication officer will record any changes made to the system. Reports of inappropriate websites or materials will be made to the ICT service immediately.

Deliberate breaches of the filtering system will be reported to the DSL/DDSL or SLT, who will escalate the matter appropriately following the relevant school policies/procedures.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL/DDSL.

20. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the ICT service. Firewalls will be switched on at all times. Staff will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the communications officer.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Staff members will be responsible for keeping their passwords private.

Users will inform the communications officer if they forget their login details. Users will not be permitted to share their login details with others and will not be allowed to log in as

another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, SLT will be informed and will decide the necessary action to take.

Users will be required to lock access to devices and systems when they are not in use.

Staff and pupils are aware that school based email and internet activity can be monitored and is traceable. If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the office manager.

21. Password security

Staff should change temporary passwords at first logon. Change passwords whenever there is any indication of possible system or password compromise. Do not record passwords or encryption keys on paper or in an unprotected file. Only disclose your personal password to authorised ICT personal in person when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished. Never tell a child or colleague your password. If you are aware of a breach of security with your password or account inform the Office Manager.

22. Emails

Staff will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. It is the responsibility of staff to keep their password secure. Staff and pupil personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email. The school email account should be the account that is used for all school business. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses. Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff should check their email regularly. Never open attachments or click on links in an email from an untrusted source and be wary of an unexpected/unusual email from a purported known source. Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

Staff will be required to block spam and junk mail, and report the matter to the communications officer. The school's monitoring system can detect inappropriate links,

malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Within the curriculum, where appropriate for pupils, they will be explicitly taught what a phishing email and other malicious emails might look like.

Pupils most likely in our secondary department, in line with their course of study will only use a school approved email account. All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.

Pupils may only use school-approved accounts on the school system and only under direct supervision for educational purposes. All emails should be written and checked carefully before sending. Pupils must immediately tell a member of staff/trusted adult if they receive an offensive email. Staff must inform a member of the senior leadership team.

23. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age and development.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

24. Social networking

The use of social media by staff and pupils will be managed by the relevant policies and procedures. The communications officer and headteacher will be responsible for all of Granta's social media platforms.

It is the expectation that staff make sure their personal social media accounts are secure and that they do not engage with any parents/carers or pupils over social media platforms. Staff will not reveal names of the school, colleagues, pupils, others or any other

confidential information acquired through your job on any social networking site or other online application.

25. The school website

The headteacher will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

26. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. All staff and where appropriate pupils will be required to adhere to device agreements (see appendices)

The office manager logs ICT equipment issued to staff and pupils and records serial numbers as part of the school's inventory. Visitors are not permitted to plug in their ICT hardware into the school network points, unless prior authorisation has been sought. Visitors are able to log into the guest wifi.

The majority of school owned devices are externally managed by the ICT service. No inappropriate apps are downloaded on to school devices and staff should be vigilant at checking the suitability of apps before downloading.

Staff must ensure that all school data is stored on the school network, and not kept solely on their issued laptop or ipad. Any equipment where personal data is likely to be stored must be encrypted, at Granta all of our personal data can be accessed through web-based systems. It is staffs' responsibility that any information accessed from personal devices is kept secure and is not disclosed to any unauthorised person.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place school devices in the boot of your car and should be taken out the car once the destination has been reached. In areas where there are likely to be members of the general public, school devices must not be left unattended, and, where possible, kept out of sight.

Equipment must be transported in its protective case, if one has been provided and should not be taken abroad without explicit permission from the Headteacher.

Staff must ensure devices are made available for necessary anti-virus updates and software installations or upgrades. Staff should never interfere with any anti-virus software installed on school ICT equipment. All files downloaded from the internet, received via e-mail or on removable media e.g. memory sticks, must be checked for any viruses using school provided anti-virus software before being used.

Personal or sensitive data should not be stored indefinitely on local drives of a desktop, laptops, USB memory stick or other portable devices. Privately owned devices are not permitted to be used on the school network.

~~The use of personal devices on the school premises and for the purposes of school work will be managed in line with the code of conduct and device agreement.~~ The school accepts no responsibility for loss or damage of a personal device.

On termination of employment, resignation or transfer, all ICT equipment should be returned to the Office Manager.

Pupils who use devices during transport to/from school that are not mobile phones, should put their devices in their bag or hand to a member of staff for safe keeping during the school day.

27. Remote learning

All remote learning will be delivered in line with the school's remote and blended learning policy.

28. Monitoring and review

The governing body, headteacher and DSL/DDSL will review this policy in full on a bi annual basis and following any online safety incidents.

Appendix A – Communication ipad parental agreement

Granta School
Cambridge Road, Linton,
Cambridge, CB21 4NN
T: 01223 896890
E: office@granta.cambs.sch.uk
W: www.granta.cambs.sch.uk
Head Teacher: Sarah Crouch



11 January 2024

Dear parent / carer,

In line with the work your child is doing at school using an iPad for communication, we are pleased that you wish to continue this work at home. We will send it home in your child's bag, please can you send it back each day so it can be used at school.

Please be aware that our school insurance does not cover the cost of equipment going home and so, in the unlikely event that it gets damaged at home, we would need to ask you to meet the costs. You might like to check that your home insurance does cover electronic items, some do but not all. Please sign and return the slip below to indicate your consent to take responsibility for the iPad when it is not on school site.

I do hope that you find this helpful and your child is able to use it to communicate more at home.

Yours Sincerely

Sarah Crouch
Headteacher

Pupils's Name:

Date:

I / we understand that when the school iPad is off school site and in the family home it is not covered by school insurance and in the event of damage occurring at home we will be required to meet the costs.

Signed.....

Appendix B – Staff laptop acceptable use agreement



Staff Laptop acceptable use agreement

This laptop is for *Work purposes only*:

You must not:

- Store personal images, videos, documents or music on your lap top.
- Let other people outside of work use your laptop (i.e. family members)
- Install/download any software including games (any unauthorised software will be removed if found). If you require any additional software, you **MUST** request this via Linda Alefounder.

You must:

- Never share your password with anyone.
- Lock your laptop when leaving it unattended.
- Store and transport your laptop in a suitable protective case and in a secure location.
- Bring your laptop into school and connected to the network to get security updates weekly (minimum).

You are responsible for the laptop and its peripherals and these would need to be in the condition that you received them in once you return them. You will be liable for any costs of lost or damaged kit.

Any damage to or faults with the equipment should be reported immediately to Linda Alefounder.

Additional information: -----

Laptop service Tag:-----

Name:-----

Signed: ----- Date: -----



Granta School
Cambridge Road, Linton,
Cambridge, CB21 4NN
T: 01223 896890
E: office@granta.cambs.sch.uk
W: www.granta.cambs.sch.uk
Head Teacher: Sarah Crouch



11 January 2024

Dear parent / carer,

As part of our Online Safety policy (which [can be found on our school website](#)) and supporting curriculum, we have devised a pupil device agreement.

We recognise that your child/young person may not understand all the elements of this device agreement. A shared commitment with yourselves will support them to be safe online and understand their actions in the most appropriate way.

We understand that your child/young person may need to use a personal device on transport, which we allow. However when in school we expect their devices to not be accessed during lesson times.

As a [school](#) we need you to support us and encourage the pupils to abide by the rules in place to keep them safe online. Your child/young person will receive education and support to stay safe online and we will support you in keeping your child/young person safe online at home.

Yours Sincerely

Sarah Crouch
~~Headteacher~~



Pupil online safety agreement

Personal safety

- I will ask permission from an adult if I want to use the internet outside of lesson times
- I will tell an adult if anything online make me feel worried, scared or upset
- I know that school will check the websites I visit
- I will check with a trusted adult that the pictures or videos I share with my friends are ok
- I will not share my personal information (my name, birthday, address, phone number, school) online.

School safety

- I will only use my log in and password and I will not tell anyone what it is
- I will not play games on a school computer, laptop or ~~ipad~~ unless a member of staff has given me permission
- I will not install software on a school computer, laptop or ~~ipad~~
- I will not use the school devices for gaming, shopping, uploading video or music

Responsibility to others

- Messages I send will be polite and responsible
- I will not upload or share images or video of another person without their permission

Personal devices

- If I bring my mobile phone or ~~ipad~~ into school. I cannot use it during lesson time.
- I will not take photos or video during the school day or on transport.

Pupil name:

