Online Safety and Acceptable Usage Policy

Date last reviewed	March 2024
Committee Responsible	Student Behaviour and Safety
Designated members of staff	Vicki Price (Associate Headteacher/DSL) Sharon Mercer (Director of Wellbeing/Deputy DSL) Deputy Headteacher (Assistant Headteacher/Technology)
Date of next review:	March 2025

CONTENTS

1. SCOPE OF THE POLICY

This policy applies to all members of the Grey Court Community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school on-line and ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place outside school. Where appropriate, incidents may be referred to outside agencies, including the Police and Children's services.

2. STATEMENT OF INTENT

Grey Court School understands that using online services is an important aspect of raising educational standards, promoting student 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 students and staff.

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

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes harm, e.g. sending and receiving explicit messages and cyberbullying.

The measures implemented to protect students 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 students and staff.

The purpose of this policy (and supporting and linked policies/documents) is to:

- set out the key principles expected of all members of the Grey Court School community with respect to the use of digital technologies
- safeguard and protect and educate the students and staff
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- define clear structures and processes to deal with inappropriate/illegal activity whilst using digital technology [noting that these need to be cross referenced with other school policies]
- minimise the risk of misplaced or malicious allegations made against adults who work with students

3. LEGAL FRAMEWORK

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes''
- DfE (2023) 'Keeping children safe in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World - 2020 edition.

4. ROLES AND RESPONSIBILITIES

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.

A whole school approach to the safe use of the internet and other digital technology involves creating a safe online learning environment which includes three main elements at Grey Court School:

- An effective range of technological tools

- Policies and procedures, with clear roles and responsibilities
- A comprehensive Online Safety Education Programme for students, staff and parents

Governors

Governors need to have an overview and understanding of online safety issues and strategies at Grey Court School. We ensure our governors are aware of guidance on online safety and are updated at least annually on policy developments.

Governors are responsible for :

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance and that it is available to all stakeholders.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an 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.
- 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 with ICT staff and service providers.
- Ensuring that the SLT 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 concern when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to online challenges and hoaxes embedded within them.

The Headteacher

The Headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL 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 annually.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping students safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The Designated Safeguarding Lead

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so that they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- 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.
- Ensuring appropriate referrals are made to external agencies, as required.
- Working closely with the police during investigations
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Ensuring that all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- 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.
- Reporting to the governing board about online safety on a termly basis.
- Working with the Headteacher and governing board to update this policy on an annual basis.

Network Manager and SLT line Manager/IT Technical Staff

The Network Manager and SLT line manager/Technical Staff are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Ensuring that the school's Acceptable Usage Policy is updated and effective and is shared with stakeholders.
- Working with the DSL and the Headteacher to conduct **half-termly** light-touch reviews of this policy.

All Staff

All staff are responsible for:

- Promoting and supporting safe behaviours in their classrooms and following the school on-line safety procedures. Central to this is fostering a 'No Blame' culture so that students feel able to report any bullying, abuse or inappropriate materials.
- 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 students 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.

Students

Students are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies. (Appendix 2).
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent information evenings, parents' evenings, a weekly e-bulletin, letters, the website, and information about national & local online safety campaigns & literature. Parents/Carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and it's Learning (VLE) and on-line student records
- their children's personal devices in the school (where this is allowed)

5. 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 the Senior Leadership Team and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about students' safety online.

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

- Staff and governors receive regular training

- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online

Handling Online Safety Concerns

Any disclosures made by students 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.

Staff will be aware that students may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that students displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The student impacted by an incident of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the student in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the child's wishes against their duty to protect the child and other young people. The DSL and other appropriate staff members will meet with the child's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the child impacted by the incident.

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, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures. If the concern is about the Headteacher, it is reported to the Chair of Governors.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates the concerns with relevant staff members, e.g. the Headteacher, Network Manager, ICT Technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police.

The school avoids unnecessarily criminalising students, 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 student 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 (the school's electronic safeguarding logging system) as outlined in the Safeguarding and Child Protection Policy.

6. CYBERBULLYING

Cyberbullying can include 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
- Menacing or upsetting responses to someone in a chatroom
- 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.

Cyberbullying against students 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.

7. CHILD-ON-CHILD SEXUAL ABUSE AND HARASSMENT

Students 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 and off and online, and will remain aware that students 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, ie. 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 students 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 be aware that interactions between the student impacted by online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other students taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy.

The school responds 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 are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child protection Policy.

8. 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 students who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The student believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The student does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The student may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the student feel 'special', particularly if the person they are talking to is older.
- The student 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 that students 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 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.
- 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 student 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 students with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

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 students at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any students displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a student relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Extremism and Radicalisation Policy and the Safeguarding and Child Protection Policy.

9. MENTAL HEALTH

The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a student's mental state, both positively and negatively. The DSL 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 student is suffering from challenges in their mental health. Concerns about the mental health of a student will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy and the Safeguarding and Child Protection Policy.

10. 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, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

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. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the student and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst students in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection Policy.

11. CYBERCRIME

Cybercrime is criminal activity committed using computers and/or the internet. There are two key categories of cybercrime:

- 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 students 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 student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cybercrime and divert them to a more positive use of their skills and interests.

The DSL and headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

12. ONLINE SAFETY TRAINING FOR STAFF AND VOLUNTEERS

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy.

The DSL ensures 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 students 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.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Safeguarding and Child Protection Policy.

13. ONLINE SAFETY AND THE CURRICULUM

The curriculum and the school's approach to online safety is developed in line with the DfE's 'Teaching Online Safety in School' guidance.

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid on-line safety risks and build their resilience.

The risks students may face online are always considered when developing the curriculum. The DSL is involved with the development of the school's online safety curriculum.

Online safety teaching is always appropriate to students' ages and developmental stages.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum; however, it is particularly addressed through:

- PDW Programme (Personal Development and Wellbeing), which includes RSHE (Relationships, Sex and Health Education)

- Computing curriculum
- Year 7 wellbeing curriculum
- Themed days and assemblies

Students 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 underpinning knowledge and behaviours students learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The DSL is involved with the development of the school's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and LAC. Relevant members of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so that these students receive the information and support they need.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for students?
- Are they appropriate for students' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure that the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the DSL considers the topic that is being covered and the potential abuse that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the class teachers on how to best support any student who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which students 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 students raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

If a student 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 Safeguarding and Child Protection Policy.

14. USE OF TECHNOLOGY IN THE CLASSROOM

A wide range of technology will be used during lessons, including computers, laptops, tablets, Internet, Email, cameras.

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students 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.

Students will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

15. 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.

Students will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the school Policy.

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

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.

Students will not be permitted to use smart devices or any other personal technology whilst in the classroom, unless directed and supervised by the teacher

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, 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.

The school will seek to ensure that it is 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 disciplinary measures.

16. REMOTE LEARNING

All remote learning will be delivered in line with the school's Remote Education Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

17. EDUCATION PARENTS/CARERS

The school works in partnership with parents to ensure students stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Parent Information evenings

- Curriculum Packs
- Home School Partnership Agreement
- Weekly eBulletin
- Letters/Emails home
- High profile events, e.g. Safer Internet Day
- Reference to the relevant web sites E publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix 4 for further links / resources)

18. TRAINING GOVERNORS

Governors should take part in online safety training sessions, with particular importance for those who are members of any subcommittee involved in technology and online safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. LGfL)
- Participation in school training and/or information sessions for staff or parents

19. FILTERING AND MONITORING ONLINE ACTIVITY

The governing board 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'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The headteacher and ICT technicians will undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements will be appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a student has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

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 who will manage the situation in line with the Child Protection and Safeguarding Policy.

20. NETWORK SECURITY

Technical security features, such as anti-virus software, will be kept up-to-date and managed by ICT technicians. Firewalls will be switched on at all times. ICT technicians will review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and students 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 ICT technicians.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Students will be provided with their own unique username and private passwords. Staff members and students will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 90 days, after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different 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, Deputy Headtaecher, i/c IT 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.

21. COMMUNICATIONS

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that the school has the ability to access any user's email account, given the Headteacher's authorisation.

- Users must immediately report, to the nominated person – in accordance with the school policy, 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.
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content:

    - These communications may only take place on official (monitored) school systems
    - Personal email addresses, text messaging or social media must not be used for these communications

- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Staff and students 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. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. 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.

Staff members and students will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect **inappropriate links, malware and** profanity within emails – staff and students will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. There will be an annual assembly where students are made aware of what a phishing email and other malicious emails might look like – this assembly will includes information on the following:

· How to determine whether an email address is legitimate

· The types of address a phishing email could use

· The importance of asking "does the email urge you to act immediately?"

· The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

22. GENERATIVE ARTIFICIAL INTELLIGENCE (AI)

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

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

The school will ensure that students 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.

23. MOBILE TECHNOLOGIES

A wide range of rapidly developing communications technologies has the potential to enhance learning. However, the school recognises that there are also a variety of associated risks which the school will ensure it manages.

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety Education programme.

- The school's Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.

- The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*No*
Internet only				*Yes*		*Yes*

24. UNSUITABLE/ INAPPROPRIATE ACTIVITIES

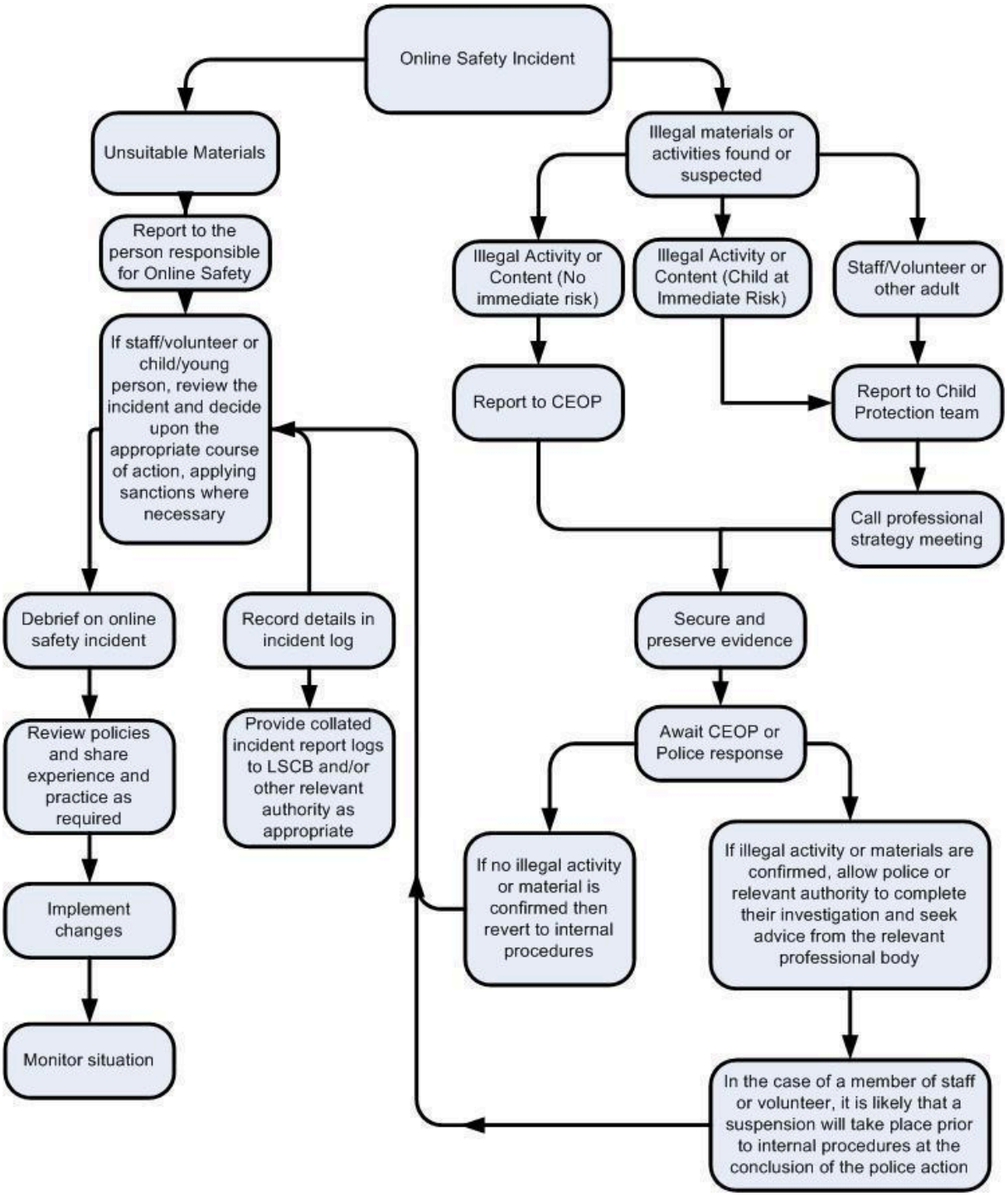
Some internet activity, e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities, e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities eg online gaming, online gambling.

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Other Incidents

It is expected that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national/local organisation (as relevant)
    - Police involvement and/or action

- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as outlined in the school Behaviour Policy.

25. LINKED POLICIES AND DOCUMENTS

This policy should be read in conjunction with:

- Remote Learning Policy
- Preventing Extremism and Radicalisation Safeguarding Policy
- General Data Protection Regulations Policy
- Allegations of Abuse Against School Staff Policy
- Low Level Safeguarding Concerns Policy
- Staff Code of conduct
- Behaviour Policy
- Relationships Policy
- Anti-bullying Policy
- Home & School in Partnership
- Personal Development and Wellbeing Statement
- Relationship Sex Education and Health Policy
- Curriculum Pack
- Twitter Guidelines
- Use of Photographs Statement
- School Technical Security Policy
- Staff Handbook

26. APPENDICES

Appendix 1: Conditions of Use of Photographs of Students

Throughout the school's academic year and your child's school life, photographs may be taken of your child. These photographs may be used in a range of contexts:
School publications, for example the prospectus
School noticeboard displays
Local newspapers as part of the media coverage of a school event
School website
Grey Court facebook and twitter pages, Grey Court Youtube channel
Internal teacher training materials and or conferences
Local education authority publications and website

If you do not want your child to appear in any photographs, please contact Ms V Price as soon as possible.

Appendix 2: Acceptable Use Policy

Grey Court expects all students to be safe and responsible when using the internet, e-mail, social networking sites or mobile phones. In particular, students must ensure that all ICT communication is respectful and sensible. Online activity, both in and outside school, must not cause distress to others, nor bring the reputation of the school into disrepute. If students come across offensive or illegal material online or within the school's systems, they should report this immediately to a member of staff. Students must understand that there are consequences to inappropriate or unacceptable use of ICT which could result in parents or the police being informed and/or suspension of access to their school ICT account.

School Network

- Students and staff are required to accept the school's AUP when logging onto the school network.
- The school network provides strictly filtered access to the internet *to support students' learning*. Student use of this service is monitored by the school. Inappropriate websites will be blocked by the school.
- Each student is provided with a secure area on our network in which to store work. Periodic random checks will be made as to the content of these files. Students found storing inappropriate material on our network may have the facility withdrawn and action taken.
- Users will not attempt to gain unauthorised access to The Grey Court School Network or go beyond their authorised access. This includes attempting to log-on through another student/staff account or access another person's files. These actions are illegal, even if only for the purposes of "browsing" or "exploring".
- An individual search will be conducted if there is reasonable suspicion that users have violated this Policy. The investigation will be reasonable and related to the suspected violation.
- Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Storage of non-school data and applications is prohibited.

Email and Internet

- The school will issue every student with an email address which they can use both in school and at home. This is a filtered service and is programmed to automatically intercept the use of swear words and other abuse or inappropriate attachments. The school will be notified if any student abuses the email system.
- Random checks of email accounts will be made as part of our monitoring procedures and students found to be using the system inappropriately will have their accounts closed and action will be taken.
- Students who repeatedly try to access game sites, ringtone providers, chat rooms and any other sites deemed to be inappropriate by the school may have their access to the internet withdrawn.
- Any student viewing adult material will automatically have their network access withdrawn and the student's parents will be notified, and further school sanctions will be applied.
- Users will not attempt to bypass the ISP filtering system. Such attempts will result in a permanent ban of Internet access and further school sanctions will be applied.

System Security:

- Users are responsible for their individual user area and should take all reasonable precautions to prevent others from being able to use it. Under no condition should users let any other student know their password.
- Users will immediately notify a teacher or the system administrator if they have identified a possible security problem. Users MUST NOT go looking for security problems because this will be construed as an illegal attempt to gain access.
- Users will avoid the inadvertent spread of computer viruses. Unchecked floppy disks and USB flash/pen drives must not be used and email attachments that are suspect or from unknown sources should not be opened.
- Users will not download computer programs or files from the Internet without permission from a member of staff.
- Users will not try to load computer programs onto the Grey Court School Network or attempt to run programs that are not accessed through the Start Menu or Desktop screen.
- Monitoring software alerts the school to inappropriate web searches by individuals. These alerts are followed up and appropriate action is taken by the school.

Misuse of Resources:

- Any student found to be tampering, damaging or otherwise abusing the School's ICT facilities will be dealt with in the strongest possible manner.
- Users will avoid unnecessary printing. A record of all printing is logged automatically by the Network. Any student found to be abusing their printing quota will have their ability to print withdrawn and will be invoiced for the excessive inks and toners used.
- Accessing and playing games via the Internet is not allowed. A limited number of games do have some significant educational value and these listed 'games' are the only ones users are permitted to access.
- For copyright reasons, users must not store or download commercial music of video files anywhere on the school network.

- Shared areas on the school network are for transferring files and users are responsible for their removal when they are no longer needed. If users place inappropriate files in a shared area then their network access is liable to be suspended.
- Listening to online radio broadcasts or watching website video clips online slows the whole network. Unless this is for educational reasons and permission has been given by a member of staff, this is not allowed.
- Users of iPads must not tamper with the settings or any application that has not been instructed for use. Misuse of the school's iPads is taken very seriously. Students found to be using them inappropriately will be banned from using them and further action will be taken.

Appendix 3: Twitter Guidelines

Personal Accounts

- Personal twitter handles must **not** include reference to Grey Court School (including acronyms and photos including the school image or logos).
- Personal twitter accounts may **not** be used to tweet photos of students or student names. These must come from your department authorised accounts (listed below).
- Personal twitter accounts can be used for professional use but should include the line – all views are my own – in your bio.

School Accounts

Authorised accounts: @GreyCourtTweets, @GreyCourtSixth, @GreyCourtArt, @GreyCourtCS, @GreyCourtDandT, @GreyCourtEngMed, @GCHumanities, @GreyCourtLib, @GreyCourtMaths, @GreyCourt_MFL, @GreyCourtPE, @GreyCourtSci, @GreyCourtAEN, @GreyCourtVPA and @GreyCourtMusic.

- Passwords
    - Current passwords for all Social Media accounts must be held by the Network Manager (YOU) and Social Media Lead (KTE)
- Naming Students
    - DO NOT use full students' names. You may use first names, a class and a photo
    - Full Names may only be used in the e:Bulletin - you may re-tweet these or send a link to articles but may not use a student's full name in a tweet
    - If you wish to use a student's full name in a tweet; winning an award, exam success etc. Please contact the parent/guardian and seek approval on a tweet by tweet basis
- Photographs
    - All students have been sent the updated photography consent agreement, including social media. SIMS keeps a record of all students who do not have consent to have their photos taken and staff will be given an updated list in July 2019
    - Staff should check the no photo list before posting any images on Social Media
    - Student names should not appear alongside photographs in external reports or publicity, unless parents have given explicit permission
- Hashtags
    - Year group hashtags are written in the format gcy followed by the year group and the year of the September they were in that year group i.e. #gcy717 should be used for the year 7s who started in September 2017

    - If you are running a trip or activity please use a hashtag of your choice starting with gc to show Grey Court. This information can then be used on letters to parents etc when advertising the trips/events
    - On the day of an event / trip please tweet @GreyCourtTweets with your hashtag
- General tweeting guidance
    - Use the School's handle (@GreyCourtTweets) to show activities/example work/ anything that's happening in your classroom. You may not receive a retweet but your tweet will come up on the school's main feed.

Appendix 4: Links to Other Organisations or Documents

Advice for Governing Bodies/Proprietors and Senior Leaders

- Childnet provide guidance for schools on cyberbullying.
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation.
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements.
- NSPCC provides advice on all aspects of a school or college's online safety arrangements.
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective.
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones.
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements.
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal

data, ensuring the content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote Education, Virtual Lessons and Live Streaming

- Case studies on remote education practice are available for schools to learn from each other.
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely.
- London Grid for Learning guidance, including platform specific advice.
- National cyber security centre guidance on choosing, configuring and deploying video conferencing.
- National cyber security centre guidance on how to set up and use video conferencing.
- UK Safer Internet Centre guidance on safe remote learning.

Support for Children

- Childline for free and confidential advice.
- UK Safer Internet Centre to report and remove harmful online content.
- CEOP for advice on making a report about online abuse.

Parental Support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support.
- Commonsensemedia provides independent reviews, age ratings, & other information about all types of media for children and their parents.
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying.
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls.
- Internet Matters provides age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world.
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation.
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online.

- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online).
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online.
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games.
- Parentzone provides help for parents and carers on how to keep their children safe online.
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations.
- UK Safer Internet Centre provides tips, advice, guides and other resources to help keep children safe online.

Appendix 5 : Online Harms and Risks - Curriculum Coverage

Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: · That age verification exists and why some online platforms ask users to verify their age · Why age restrictions exist · That content that requires age verification can be damaging to under-age consumers · What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: <u>PDW</u> Year 7 - Digital Privacy Year 9 - Socialising online Year - Online safety Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world <u>Wellbeing</u> Year 7 - Online Safety <u>Computing</u> Year 7 - Welcome and introduction to school systems Year 9 - Cyber Security KS4 - iDEA platform

How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: · What a digital footprint is, how it develops and how it can affect students' futures · How cookies work · How content can be shared, tagged and traced · How difficult it is to remove something once it has been shared online · What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: RSE (PDW) Year 9 - Socialising online Year - Online safety Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world Computing Year 7 - Welcome and introduction to school systems Year 9 - Cyber Security KS4 iDEA Platform

Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: · Disinformation and why individuals or groups choose to share false information in order to deliberately deceive · Misinformation and being aware that false and misleading information can be shared inadvertently · Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons · That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online · How to measure and check authenticity online · The potential consequences of sharing information that may not be true	This risk or harm is covered in the following curriculum areas: RSE (PDW) Computing <u>Citizenship (PDW)</u> Year 8 - British Values Year 9 - Socialising online Year 10 - Extremism and Radicalisation Year 11 - Living in the Wider world <u>Wellbeing</u> Year 7 - Online Safety <u>Computing</u> Safer internet day - all year groups Year 7 - Welcome and introduction to school systems Year 9 - Cyber Security KS4 iDEA Platform

Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: · How to recognise fake URLs and websites · What secure markings on websites are and how to assess the sources of emails · The risks of entering information to a website which is not secure · What students should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email · Who students should go to for support	This risk or harm is covered in the following curriculum areas: <u>RSHE (PDW)</u> Year 9 - Socialising online Year 10 - Extremism and Radicalisation <u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: · What identity fraud, scams and phishing are · That children are sometimes targeted to access adults' data · What 'good' companies will and will not do when it comes to personal details	<u>PDW</u> Year 9 - Socialising online Year 10 - Financial Education <u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform

Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: · Why passwords are important, how to keep them safe and that others might try to get people to reveal them · How to recognise phishing scams · The importance of online security to protect against viruses that are designed to gain access to password information · What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum areas: <u>PDW</u> Safer internet day <u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform KS4 1.4 Network Security
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: · How cookies work · How data is farmed from sources which look neutral · How and why personal data is shared by online companies · How students can protect themselves and that acting quickly is essential when something happens · The rights children have with regards to their data · How to limit the data companies can gather	<u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform KS4 1.6 Legislation

Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: · That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible · How notifications are used to pull users back online	<u>PDW</u> Year 7 - The Media and Democracy Year 11 - The Instagram effect <u>Computing</u> Safer internet day - all year groups KS4 iDEA Platform
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: · How to find information about privacy settings on various devices and platforms · That privacy settings have limitations	<u>Computing</u> KS4 iDEA Platform
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: · How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts · How the targeting is done · The concept of clickbait and how companies can use it to draw people to their sites and services	<u>PDW</u> Year 9 - Socialising online <u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform

Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: · The types of online abuse, including sexual harassment, bullying, trolling and intimidation · When online abuse can become illegal · How to respond to online abuse and how to access support · How to respond when the abuse is anonymous · The potential implications of online abuse · What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: <u>PDW</u> Year 7 - Digital Privacy Year 9 - Socialising online Year - Online safety Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world <u>Wellbeing</u> Year 7 - Online Safety <u>Computing</u> Year 9 - Cyber Security KS4 iDEA Platform KS4 1.6 Legislation

Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: · What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal · How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why · That it is okay to say no and to not take part in a challenge · How and where to go for help · The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	<u>Computing</u> KS4 iDEA Platform
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: · That online content (sometimes gang related) can glamorise the possession of weapons and drugs · That to intentionally encourage or assist in an offence is also a criminal offence · How and where to get help if they are worried about involvement in violence	RSE (PDW) PDW Computing <u>PDW</u> Year - Online safety Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world Year 11 - Gangs <u>Safer internet day - all year groups</u>

Fake profiles	Not everyone online is who they say they are. Teaching includes the following: · That, in some cases, profiles may be people posing as someone they are not or may be 'bots' · How to look out for fake profiles	RSE (PDW) Year 7 - Digital Privacy Year 9 - Socialising online Year 10 - Online Safety inc nudes/sexting <u>Wellbeing</u> Year 7 - Online Safety <u>Computing</u> Year 7 - Introduction to school systems Year 7 - Digital Skills KS4 - iDEA platform
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: · Boundaries in friendships with peers, in families, and with others · Key indicators of grooming behaviour · The importance of disengaging from contact with suspected grooming and telling a trusted adult · How and where to report grooming both in school and to the police At all stages, it is important to balance teaching students about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	<u>RSE(PDW)</u> Year 7 - Digital Privacy Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety including nudes/sexting Year 11 - Living in the Wider world

		Wellbeing Year 7 - Online Safety Safer Internet Day - all year groups Computing Year 9 - Cyber Security KS4 iDEA Platform
Live Streaming	Live Streaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: · What the risks of carrying out livestreaming are, e.g. the potential for people to record live streams and share the content · The importance of thinking carefully about who the audience might be and if students would be comfortable with whatever they are streaming being shared widely · That online behaviours should mirror offline behaviours and that this should be considered when making a livestream · That students should not feel pressured to do something online that they would not do offline · Why people sometimes do and say things online that they would never consider appropriate offline · The risk of watching videos that are being live streamed, e.g. there is no way of knowing what will be shown next · The risks of grooming	RSE (PDW) Year 7 - Digital Privacy Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world Wellbeing Year 7 - Online Safety Safer Internet Day - all year groups Computing KS4 iDEA Platform

Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: · That pornography is not an accurate portrayal of adult sexual relationships · That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour · That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work	RSE (PDW) Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety inc nudes/sexting Year 11 - Sex and Relationships <u>Wellbeing</u> Year 7 - Online Safety <u>Safer Internet Day - all year groups</u>

Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: · That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with · How to identify indicators of risk and unsafe communications · The risks associated with giving out addresses, phone numbers or email addresses to people students do not know, or arranging to meet someone they have not met before · What online consent is and how to develop strategies to confidently say no to both friends and strangers online	RSE(PDW) Year 7 - Digital Privacy Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world <u>Wellbeing</u> Year 7 - Online Safety <u>Safer Internet Day - all year groups</u> <u>Computing</u> Year 7 - Digital Skills Year 9 - Cyber Security KS4 iDEA Platform

Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: · The issue of using image filters and digital enhancement · The role of social media influencers, including that they are paid to influence the behaviour of their followers · The issue of photo manipulation, including why people do it and how to look out for it	RSE (PDW) Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety inc nudes/sexting Year 11 - Sex and Relationships <u>Wellbeing</u> Year 7 - Online Safety <u>Safer Internet Day - all year groups</u> PDW

Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: · How to evaluate critically what students are doing online, why they are doing it and for how long (screen time) · How to consider quality vs. quantity of online activity · The need for students to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear of missing out · That time spent online gives users less time to do other activities, which can lead some users to become physically inactive · The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues · That isolation and loneliness can affect students and that it is very important for them to discuss their feelings with an adult and seek support · Where to get help	RSE (PDW) Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Sex and Relationships Year 10 - Sex and Relationships Year 11 - Sex and Relationships <u>Safer Internet Day - all year groups</u> PDW Year 7-11 - Mental Health incorporated into most PDW SOWs
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: · How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives · How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	RSE (PDW) Year 7 - Digital Privacy Year 7 - Sex and Relationships Year 8 - Sex and Relationships Year 9 - Socialising Year 9 - Sex and Relationships

		Year 10 - Body Image Year 10 - Extremism and Radicalisation Year 10 - Online Safety inc nudes/sexting Year 11 - Living in the Wider world <u>Wellbeing</u> Year 7 - Online Safety <u>Safer Internet Day - all year groups</u> <u>Computing</u> Year 7 - Digital Skills Year 9 - Cyber Security KS4 iDEA Platform
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: · Strategies for positive use · How to build a professional online profile	<u>PDW</u> Year 9 - Careers Year 11 - Careers <u>Computing</u> KS4 iDEA Platform
Suicide, self-harm and eating disorders	Students may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for students and should take care to avoid giving instructions or methods and avoid using language, videos and images.	PDW Year 7-11 - Body image incorporated into every year group's SOW