



**Greys
Education
Centre**

Aspirational • Collaborating



**Bedford Inclusive Learning
and Training Trust**

Achieving • Believing • Collaborating

Online Safety Policy

Greys Education Centre

Policy Status: Other

Review Cycle: Two Yearly

Owner: Catherine Assink

Date: July 2025

Approved by: Trust Board

Date: July 2025

Review Date: July 2027

Our commitment

BILTT is committed to ensuring safer lives and excellent learning for all children and young people. As we increasingly work, learn and teach online, it is essential that children are safeguarded from potentially harmful and inappropriate online material.

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. Please see Appendix 2: Specific safeguarding issues related to online safety.

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Accordingly, we have appropriate internet filtering and monitoring within each academy and our central services. The welfare and safety of each individual child is paramount and therefore we are committed to providing a safe online learning environment by:

- ensuring robust processes are in place to ensure the online safety of pupils, staff, volunteers and governors.
- delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education \(updated September 2024\)](#) and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the [DfE's filtering and monitoring standards](#) and the Department's Prevent guidance on [protecting children from radicalisation](#)

This policy reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

We also follow the online safety guidance as recommended within Keeping Children Safe in Education within our delivery of remote education, virtual lessons and live streaming. This includes a

range of resources and guidance (Appendix 1 - Useful links and resources for staff, pupils and parents)

Roles and responsibilities

The BILTT Board of Trustees

The Board of Trustees is responsible for approving the Online Safety Policy Template.

The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The LGB will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs/electronic records as provided by the academy designated safeguarding lead (DSL).

All governors will:

- a) Ensure that they have read and understood this policy
- b) Sign to confirm they agree and will adhere to the terms on acceptable use as detailed in the ICT Acceptable Use Policy
- c) Governors ensure that pupils are taught about safeguarding, including online, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach
- d) Ensure the DSL takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role
- e) Ensure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training
- f) Review the DfE's filtering and monitoring standards and ensure the school is meeting them

The Headteacher

The academy Headteacher is responsible for:

- a) ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- b) ensuring that all staff sign to agree and adhere to the ICT Acceptable Use Policy.
- c) Assure and ensure the work of the academy DSL in monitoring pupils' online behaviour and knowledge, and take appropriate action if necessary.

The academy Designated Safeguarding Lead

Details of the academy's designated safeguarding lead (DSL) are set out in our Safeguarding Policy. The DSL takes lead responsibility for online safety in school, in particular:

- a) Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- b) Working with the Headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- c) Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- d) Ensuring that any incidents of cyberbullying, online child on child abuse, including sexual harassment and the sending of 'nudes', are logged and dealt with appropriately in line with the school behaviour policy
- e) Updating and delivering staff training on online safety
- f) Liaising with other agencies and/or external services as necessary
- g) Providing regular reports on online safety in school to the Headteacher, Trust DSL, CEO, and/or those responsible for governance
- h) Monitoring online safety reports ~~where designated to do so~~ and taking appropriate action.
- i) Conduct an annual review of our filtering and monitoring provision along with the IT Lead, member of SLT and designated Trustee member
- j) Check that our current filtering and monitoring system blocks harmful and inappropriate content without unreasonably impacting teaching and learning
- k) Composing and reviewing regularly the:
 - [Online safety curriculum overview](#)
 - [Pupil online safety agreement](#)
 - [Pupil agreement: Use of mobile phones](#)

The academy IT manager/lead

The IT manager/lead is responsible for:

- a) Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- b) Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- c) Blocking access to potentially dangerous sites and, preventing the downloading of potentially dangerous files
- d) Ensuring that any incidents of cyberbullying, online peer on peer abuse, including sexual harassment and the sending of 'nudes', are logged and dealt with appropriately in line with the school behaviour policy.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers will be vigilant to ensure the safe use of online technology and be particularly aware that our pupils, all of which have SEND, are at greater risk of radicalisation as detailed in our Safeguarding Policy. Staff are responsible for:

- a) Maintaining an understanding this policy
- b) Implementing this policy consistently
- c) Signing to show their agreement and intention to adhere to the terms of the ICT Acceptable Use Policy and ensuring that pupils follow the academy's Pupil online safety agreement
- d) Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
- e) Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school behaviour policy.
- f) To understand their expectations, roles and responsibilities around filtering and monitoring
- g) Report concerns regarding online safety and filtering and monitoring to the DSL via sharepoint online forms

Designated Safeguarding Lead (DSL) and deputy DSL

Academy DSLs/DDSLs will:

- a) Provide opportunities to share best practice with each other and securing effective training (e.g. NSPCC and Child Exploitation Online Protection)
- b) Provide regular updates and resources
- c) Provide support and guidance on specific matters relating to online safety as appropriate.

Parents

Parents are expected to:

- a) Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- b) Ensure their child has read, understood and agreed to the terms of the academy's [Pupil online safety agreement](#)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- a) What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- b) Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- c) Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>
- d) Think U Know - resources and information by the National Crime Agency: <https://www.thinkuknow.co.uk/>
- e) Resources and information from the NSPCC: [Net Aware](#)

Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the ICT Acceptable Use Policy

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum. We educate pupils about online safety at an age and cognition appropriate level and in accordance with DfE guidance as outlined in: [Teaching pupils about online safety](#)

The safe use of social media and the internet will also be covered in other subjects where relevant.

The academy will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite relevant speakers to present to pupils.

Educating parents about online safety

The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on our website.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Please note, Appendix 1: Useful links and resources for staff, pupils and parents.

Cyberbullying

Definition

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

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victims.

With due regard for pupils cognition, the academy will actively discuss cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes when appropriate, and the issue will be addressed in assemblies.

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

- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The academy also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
- See also appendix 2: Specific safeguarding issues related to online safety for information relating to other online safeguarding issues.

Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- a) Cause harm, and/or
- b) Disrupt teaching, and/or
- c) Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- a) Delete that material, or
- b) Retain it as evidence (of a criminal offence or a breach of school discipline)
- c) Report it to the police

Any searching of pupils must be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

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

Acceptable use of the internet in the academy

All staff, volunteers and governors annually affirm their agreement regarding the acceptable use of the academy's IT systems and the internet through the Code of Conduct.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in the academy:

Pupils may bring mobile devices into the academy, however at the Secondary site, these must be handed in, to the office in the morning and they will be returned at the end of the school day.

We recognise that children are capable of abusing their peers, including but not limited to, bullying, cyberbullying and sexting. We are well informed with regards to the guidance within Keeping Children Safe in Education in recognising and dealing with instances of such abuse and this behaviour will not be tolerated.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy

Staff using work devices outside of the academy

Staff members using a work device outside of the academy must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use, as set out in the ICT Acceptable Use Policy.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of the academy. Any USB devices containing data relating to the school must be encrypted.

How the academy will respond to issues of misuse

Where a pupil misuses the academy's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents should be reported to the police.

Training

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

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

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

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

Monitoring arrangements

The DSL (and deputy/deputies)) monitor behaviour and safeguarding issues related to online safety including any monitoring notifications from filtering software.

Links with other policies

This online safety policy is linked to the following policies:

Safeguarding

Mental Health & Wellbeing

Acceptable Use

Behaviour

Health and Safety

Anti-bullying

Code of Conduct

Data Protection

Use of Images of Children

RSHE

Appendix 1: Useful links and resources for staff, pupils and parents

Opportunities to teach online safety to pupils

- [Be Internet Legends](#) developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- [Disrespect nobody](#) is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- [Education for a connected world](#) framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- [PSHE association](#) provides guidance to schools on developing their PSHE curriculum
- [Teaching online safety](#) in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- [Thinkuknow](#) is the National Crime Agency/CEOPs education programme with age specific resources
- [Sexting: responding to incidents and safeguarding children](#) - UK Council for Internet Safety. UK Safer Internet Centre has developed further guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

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
- [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 [sexting-in-schools-andcolleges](#) and [using-external-visitors-to-support-online-safety-education](#)

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](#) provide 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](#) provide 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
- [Lucy Faithfull Foundation StopItNow](#) resource 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](#) provide tips, advice, guides and other resources to help

Appendix 2: Specific safeguarding issues related to online safety

Cyberbullying

Cyberbullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Cyberbullying can also be a form of peer on peer abuse through sexual harassment that happens through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.

Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy actively discusses cyberbullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyberbullying with their classes when appropriate, and the issue will be addressed in assemblies.

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

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

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

In relation to a specific incident of cyber-bullying, the academy will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk is part of our safeguarding approach.

We are particularly vigilant to any online behaviour that suggests any radicalised behaviour through monitoring of internet use.

Extremism

Extremism goes beyond terrorism and is defined as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces (As defined in the Government's Counter Extremism Strategy). Extremists often target the vulnerable - including the young- by seeking to sow divisions between communities on the

basis of race, faith or denomination; justifying discrimination towards women and girls; seeking to persuade others that minorities are inferior; or arguing against the primacy of democracy and the rule of law in our society.

Radicalisation

Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability.

Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.

As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. Staff should use their judgement in identifying children who might be at risk of radicalisation and act proportionately which may include the designated safeguarding lead (or deputy) making a referral to the Channel programme.

The Prevent duty

All schools and colleges are subject to a duty under section 26 of the CounterTerrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".

This duty is known as the Prevent duty. The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the Revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76 which are specifically concerned with schools (and also covers childcare). The guidance is set out in terms of four general themes: Risk assessment, working in partnership, staff training, and IT policies. Schools have a duty to prevent children from being drawn into terrorism. The DSL will undertake Prevent awareness training and make sure that staff have access to appropriate training to equip them to identify children at risk.

We will assess the risk of children in our school being drawn into terrorism. This assessment will be based on an understanding of the potential risk in our local area, in collaboration with our local safeguarding children board and local police force.

We will ensure that suitable internet filtering is in place and equip all pupils to stay safe online at school and at home.

There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. Radicalisation can occur quickly or over a long period. Staff will be alert to changes in pupils' behaviour to ensure early identification of risk.

The government website [Educate Against Hate](#) and charity [NSPCC](#) say that signs that a pupil is being radicalised can include:

- Refusal to engage with, or becoming abusive to peers who are different from themselves
- Becoming susceptible to conspiracy theories and feelings of Persecution
- Changes in friendship groups and appearance

- Rejecting activities they used to enjoy
- Converting to a new religion
- Isolating themselves from family and friends
- Talking as if from a scripted speech
- An unwillingness or inability to discuss their views
- A sudden disrespectful attitude towards others
- Increased levels of anger
- Increased secretiveness, especially around internet use
- Expressions of sympathy for extremist ideologies and groups, or justification of their actions
- Possessing extremist literature
- Being in contact with extremist recruiters and joining, or seeking to join, extremist organisations

Children who are at risk of radicalisation may have low self-esteem, or be victims of bullying or discrimination.

It is important to note that these signs can also be part of normal teenage behaviour – staff should have confidence in their instincts and seek advice if something feels wrong.

If staff are concerned about a pupil, they will follow our procedures set out in this policy, including discussing their concerns with the DSL. Staff should always take action if they are worried. Further information on the school's measures to prevent radicalisation are set out in other school policies and procedures.

Additional support:

The department has published advice for schools on the Prevent duty. to complement the Prevent guidance and signposts other sources of advice and support. Prevent duty guidance: for further education institutions in England and Wales that applies to colleges. Educate Against Hate, a website launched by Her Majesty's Government has been developed to support and equip school and college leaders, teachers, and parents with information, tools and resources (including on the promotion of fundamental British values) to help recognise and address extremism and radicalisation in young people. The platform provides information on and access to training resources for teachers, staff and school and college leaders, some of which are free such as Prevent e-learning, via the Prevent Training catalogue.

Channel:

Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. It provides a mechanism for schools to make referrals if they are concerned that an individual might be vulnerable to radicalisation. An individual's engagement with the programme is entirely voluntary at all stages. Guidance on Channel is available [here](#)

The school or college's Designated Safeguarding Lead (and any deputies) should be aware of local procedures for making a Channel referral.

As a Channel partner, the school or college may be asked to attend a Channel panel to discuss the individual referred to determine whether they are vulnerable to being drawn into terrorism and consider the appropriate support required.

Contextual factors:

Safeguarding incidents and/or behaviours can be associated with factors outside the academy /or can occur between children outside the school or college. This can involve violent, humiliating and degrading sexual assaults, but does not always involve physical contact and can happen through the use of technology online. For example, young people may be persuaded or forced to share sexually explicit images of themselves, have sexual conversations by text, or take part in sexual activities using a webcam.

All staff, but especially the designated safeguarding lead (or deputy) should be considering the context within which such incidents and/or behaviours occur. This is known as contextual safeguarding, which simply means assessments of children should consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare.

Children's social care assessments should consider such factors so it is important that schools and colleges provide as much information as possible as part of the referral process. This will allow any assessment to consider all the available evidence and the full context of any abuse.

Greys education centre online-safety policy

Introduction

Key people / dates

Designated Safeguarding Lead (DSL) team	Jo Tift Jo.tift@biltt.org
Online-safety lead (if different)	As Above
Online-safety / safeguarding link governor	
PSHE/RSHE lead	Chantelle Di'Iorio Chantelle.lorio@biltt.org
Network manager / other technical support	Paul Panter Paul.panter@biltt.org
Date this policy was reviewed and by whom	September 2025 Cain Gentle King Kyle Lawrence
Date of next review and by whom	July 2025 (Greys LGB)

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'in line with the Online Safety Act 2023, Keeping Children Safe in Education 2025 (KCSIE), and relevant Ofcom guidance (2024–25). It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside your school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, you should involve staff, governors, pupils and parents in writing and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand, or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

You may have a named online-safety lead at your school (see above); this person may or may not be the designated safeguarding lead (DSL), but KCSIE makes clear that “the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report “Safer children in a digital world”). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three. Many of these new risks are mentioned in KCSIE 2019, e.g. fake news, upskirting and sticky design.

The LGfL DigiSafe 2018 pupil survey of 40,000 pupils identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on ‘stranger danger’, i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

Following the Online Safety Act 2023, primary pupils must be actively protected from harmful or age-inappropriate content online. Our school recognises the importance of regulating access to algorithms, harmful social media trends, and sexually explicit content through clear age-appropriate filtering and safe digital zones.

Staff are supported to teach about:

- Age-appropriate content boundaries
- In-app and online reporting tools
- Respectful online behaviour and reporting sexual harassment, bullying or abuse

Our online safety strategy reflects that many children in KS2 are accessing platforms with a minimum age of 13 or above. We do not encourage this use but equip children to be resilient if exposed.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review

- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement
- Aligned with the duties of the Online Safety Act, this policy is reviewed annually to reflect new Ofcom safety codes, particularly relating to protections for primary-aged children online

Overview

Aims

This policy aims to:

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

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Scope

This policy applies to all members of the Greys Education Centre community (including staff, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and responsibilities

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

the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Headteacher/Principal – Vanessa Millar

Key responsibilities:

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

Designated Safeguarding Lead / Online Safety Lead – Jo Tiff

Key responsibilities (remember the DSL can delegate certain online-safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2019):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and

establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”

- “Liaise with the local authority and work with other agencies in line with Working together to safeguard children”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework ‘Education for a Connected World’) and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this).
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff:
 - all staff must read KCSIE Part 1 and all those working with children Annex A
 - it would also be advisable for all staff to be aware of Annex C (online safety)
 - cascade knowledge of risks and opportunities throughout the organisation
 -

In addition, the DSL will ensure that the school complies with current statutory duties under the Online Safety Act 2023, including:

- Carrying out risk assessments of digital platforms and online tools used in school.
- Ensuring that filtering and monitoring systems are appropriate for children under 13.
- Making sure that staff and pupil training includes awareness of new and emerging risks such as harmful online trends, deepfakes, and AI-generated content.

Governing Body, led by Online Safety / Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2025):

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#)
- “Ensure an appropriate **senior member** of staff, from the school or college leadership team, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support...”
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- “Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated [...] in line with advice from the local three safeguarding partners [...] integrated, aligned and considered as part of the overarching safeguarding approach.”
- “Ensure appropriate filters and appropriate monitoring systems are in place [but...] be careful that ‘overblocking’ does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding”.
- “Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology.” NB – you may wish to refer to ‘Teaching Online Safety in Schools 2019’ and investigate/adopt the UKCIS cross-curricular framework ‘Education for a Connected World’ to support a whole-school approach

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.

- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook.
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new DfE document on this)
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Be aware of platform age restrictions and how to educate children about using age-appropriate games, apps, and sites in line with the Online Safety Act 2023

PSHE / RSHE Lead/s – Chantelle Di'orio

Responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and

securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.

Computing Lead – Kyle Lawrence / Cain Gentle-King

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager/technician – Paul Panter

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

- Work with the Headteacher to ensure the school website meets statutory DfE requirements (see appendices for website audit document)

Data Protection Officer (DPO) – Julie Connor

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology

- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- NB: the LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety (but only half talk about it with them more than once a year).

Parents are supported to understand the key elements of the Online Safety Act that apply to primary-aged children, particularly around:

- Age restrictions on platforms and games
- Age-verification tools coming into force in 2025
- Reporting routes if children encounter harmful online content
- School-run workshops and newsletters include information aligned to Ofcom's "Media Literacy" guidance for families.

Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- PSHE
- Relationships education, relationships and sex education (RSE) and health
- Computing
- Citizenship

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age

appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Greys Education Centre, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety.)

In line with the Online Safety Act 2023, our curriculum includes direct teaching about:

- How to report harmful or worrying online content
- How to recognise age-appropriate content
- Understanding the risks of in-game chat, streaming, and algorithmically suggested videos

Staff are supported through CPD to meet new statutory expectations for online safeguarding education in primary settings.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; Where age-restricted or harmful content is accessed by children, staff must log the incident and refer it to the DSL. This is particularly important if children encounter material relating to pornography, self-harm, or violent content, as covered under the Online Safety Act. The DSL will assess whether to report to relevant external bodies (e.g. CEOP, Internet Watch Foundation, Ofcom). Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / child on child Abuse Policy (if separate)
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies

- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

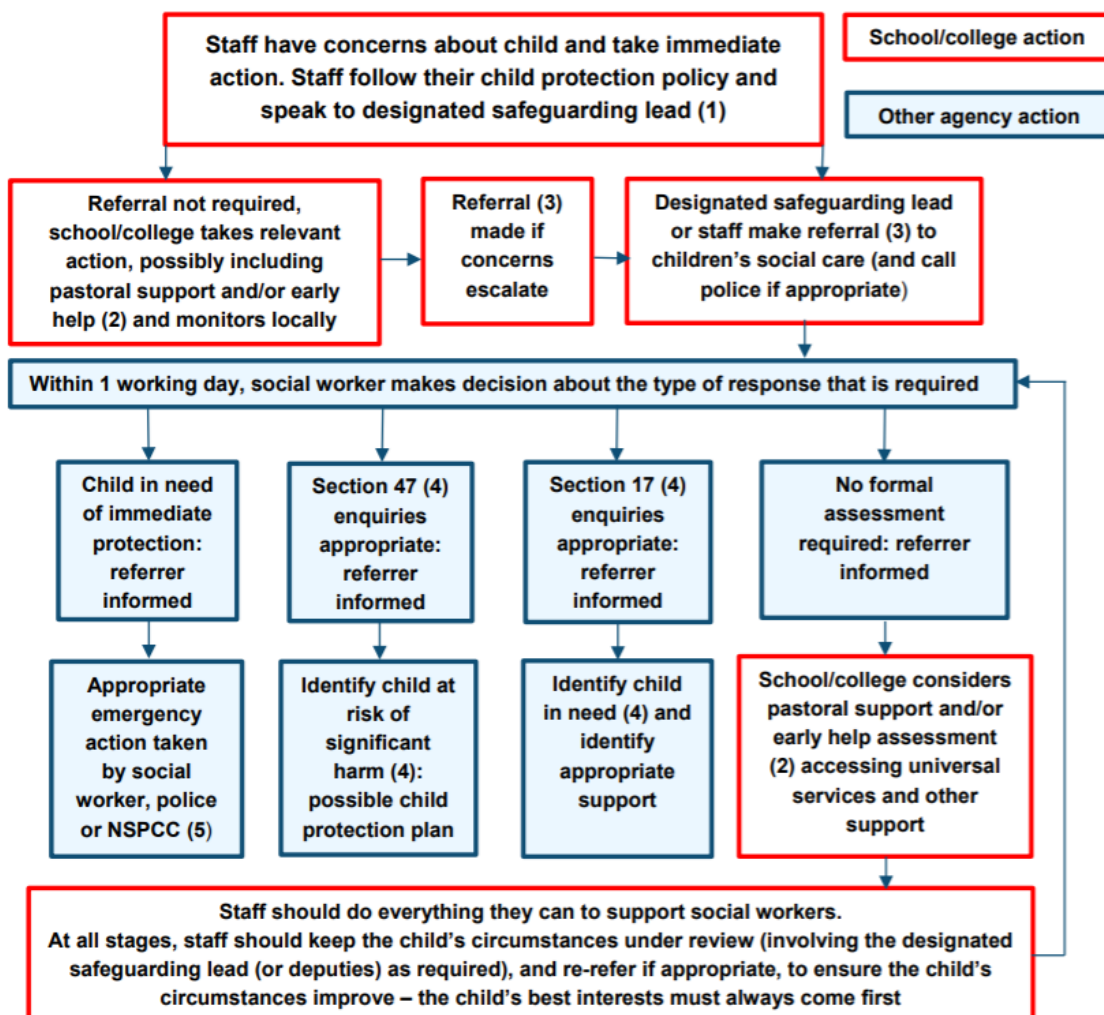
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

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

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Actions where there are concerns about a child

The following flow chart (it cannot be edited) is taken from page 13 of Keeping Children Safe in Education 2019 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(1) In cases which also involve a concern or an allegation of abuse against a staff member, see Part Four of this guidance.

(2) Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Chapter one of [Working Together to Safeguard Children](#) provides detailed guidance on the early help process.

(3) Referrals should follow the process set out in the local threshold document and local protocol for assessment. Chapter one of [Working Together to Safeguard Children](#).

(4) Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Chapter one of [Working Together to Safeguard Children](#).

(5) This could include applying for an Emergency Protection Order (EPO).

Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sexting; how to respond to an incident](#) for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, [Sexting in Schools and Colleges](#) to decide next steps and whether other agencies need to be involved.

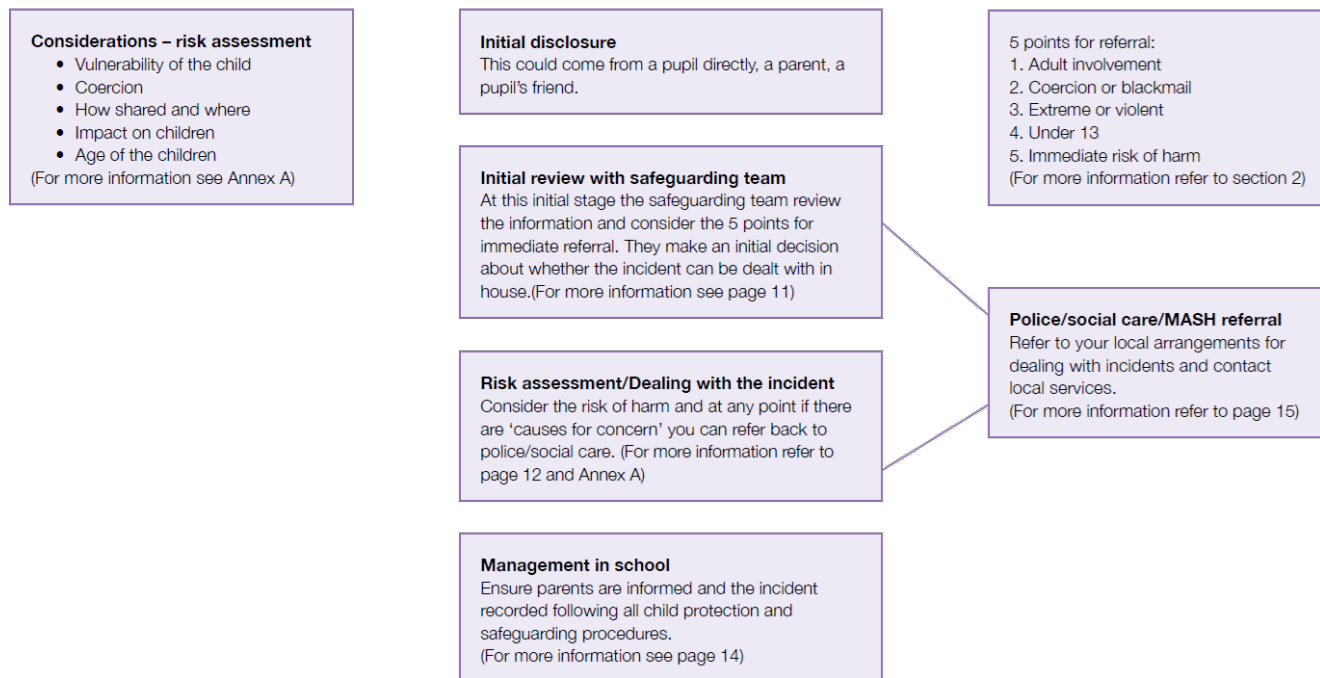
It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

Annex G

Flowchart for responding to incidents



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

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. [Click here to view our Behaviour Policy.](#)

Sexual violence and harassment

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

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

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

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

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Greys Education Centre community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Greys Education Centre will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection:

a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements, [click here to view these policies](#).

The headteacher/principal, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Smartware to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

Appropriate filtering and monitoring

In line with the Online Safety Act 2023 and Keeping Children Safe in Education (KCSIE) 2024, primary schools have a duty to protect pupils from online harm. This includes:

- Using verified, age-appropriate filtering systems that block access to harmful or adult content (such as pornography, violence, and age-restricted platforms).
- Implementing monitoring tools that highlight searches or activity linked to self-harm, bullying, sexual exploitation, or violence.
- Having clear procedures to record, review, and respond to online safety incidents and risks across all key stages.

At Greys Education Centre, our filtering and monitoring systems meet Ofcom's technical standards under the Online Safety Act. We ensure pupils cannot access harmful or inappropriate material, while also taking care to avoid "over-blocking" that might unnecessarily restrict safe and important teaching or safeguarding content.

Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Pupils at this school use the Microsoft Outlook for their emailing system.
- Staff at this school also use the Microsoft Outlook system for all school emails.

Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
 - If data needs to be shared with external agencies, encryption is needed.
 - Internally, staff should use the school network, including when working from home when remote access is available via the Office365 system.
- Pupils have access to their emails through the Office 365 system.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Pupils and staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

See also the social media section of this policy.

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Principal and Governors have delegated has been the day-to-day responsibility of updating the content of the website to Sally Bradshaw. The site is also managed by Sally Bradshaw.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with Sally Bradshaw.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the DfE document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)'.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – [see our DP policy here](#).

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush – never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

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

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high profile image for display or publication

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name.

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

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

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

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

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

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

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

Social media

Greys Education Centre's SM presence

Greys Education Centre works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online (Mumsnet is a favourite).

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner, even though at current, there are no official/active school social media accounts.

Staff, pupils' and parents' SM presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school

community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

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

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

In light of the Online Safety Act, we are preparing children to understand age-appropriate platform use, how to avoid risky sharing behaviour, and how to respond if they encounter inappropriate messages or content. This includes how to report content to platforms and seek support from trusted adults

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this (as outlined on p.15) by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

It is encouraging that 73% of pupils (from the 40,000 who answered that LGfL DigiSafe pupil online safety survey) trust their parents on online safety (although only half talk about it with them more than once a year at the moment).

Email is the official electronic communication channel between parents and the school, and between staff and pupils (see page 32 for full details).

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 33) and permission is sought before uploading photographs, videos or any other information about other people.

Device usage

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils/students** are allowed to bring mobile phones in to school, however, these must be handed in at reception in the morning and stored safely and collected at home time.
- The school reinforces that devices brought from home must not have access to age-inappropriate apps (e.g. TikTok, Snapchat, Discord) or browsers without filtering. From 2025, legal changes may require parents to use age-verification apps and controls at home, and the school will support families in navigating this.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page 33 and Data protection and data security section on page 30. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page 33. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

Pupils/students are not allowed networked file access via personal devices.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section on page 33 and Data protection and data security section on page 30. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.

Trips / events away from school

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

Searching and confiscation

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

Appendices

1. Safeguarding Incident log
2. Safeguarding and Child Protection Policy [Click here to view the Safeguarding Policy](#)
3. Behaviour Policy / Anti-Bullying Policy
4. Staff Code of Conduct / Handbook
5. *Acceptable Use Policies (AUPs) for:
 - *Pupils
 - *Staff, Volunteers Governors & Contractors
 - *Parents
6. *Letter to parents about filming/photographing/streaming school events
7. *Prevent Risk Assessment Template
8. *E-Security Policy
9. *Online-Safety Questions from the Governing Board (UKCIS)
10. *Education for a Connected World cross-curricular digital resilience framework (UKCIS)
11. *Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
12. *Working together to safeguard children (DfE)
13. *Searching, screening and confiscation advice (DfE)
14. *Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
15. *Sexting guidance from UKCIS
 - *Overview for all staff
 - *Full guidance for school DSLs
16. *Prevent Duty Guidance for Schools (DfE and Home Office documents)
17. *Data protection and data security advice, procedures etc
18. *Preventing and tackling bullying (DfE)
19. Cyber bullying: advice for headteachers and school staff (DfE)
20. *RAG (red-amber-green) audits for statutory requirements of school websites