



**Grange
Academy**
Belong • Believe • Achieve



**Bedford Inclusive Learning
and Training Trust**
Achieving • Believing • Collaborating

Online Safety Policy

Grange Academy

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 \(updated Jan 2021-September 2024\)](#) 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: (Adapt this section to reflect your academy's approach)

Pupils may bring mobile devices into the academy, but are not permitted to use them during:

- a) Lessons or assemblies or any other educational activity
- b) Clubs before or after school, or any other activities organised by the academy.

Any use of mobile devices in school by pupils must be in line with the <Pupil agreement: Use of mobile phones>, particularly those devices with internet access.

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.

This also refers to the practice of 'upskirting', which has been made a criminal offence under the Voyeurism Act 2019. This practice *'typically involves taking a picture under a person's clothing without them knowing with the specific intention of viewing their genitals or buttocks to gain sexual gratification, or cause the victim humiliation, distress or alarm'*.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the academy behaviour policy, which may result in the confiscation of their device.

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
- [Disrespectnobody](#) 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.

Appendix 3

Grange Academy

ONLINE SAFETY CURRICULUM OVERVIEW

Curriculum intent:

At Grange Academy, it is our intention that our pupils are well equipped with an online safety curriculum that is relevant, and purposeful and provides pupils with the necessary knowledge and skills to keep themselves safe whilst using technology. To deliver our curriculum, we use the PSHE Association Framework, Poled resources and Education for a Connected World Framework as a planning tool for lesson delivery, along with considering the needs and abilities of our pupils.

Our planning and delivery is progressive, to ensure that online safety is taught as a prerequisite and then woven in line with our Computing and RSHE curriculum, to give an optimum impact. Online safety coverage is carefully planned within the context of our safeguarding duty taught in school, to ensure that all pupils understand the core element of keeping themselves safe.

Where necessary, pupils will have targeted intervention to further enhance protective behaviours.

Breadth of Study:

- Personal, social and emotional development: Managing self
- Use technology safely and respectfully
- Keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Use technology safely and respectfully, and responsibly
- Recognise acceptable and unacceptable behaviours online
- Keeping personal information private
- Identify a range of ways to report concerns about content and contact

Whole school coverage:

The following grid shows the coverage of Online Safety taught across the school. Each topic has been carefully and progressively planned to build upon pupils' knowledge and skills. Within each lesson, pupils learn about different aspects of online safety, appropriate to their level of need. These are built upon progressively over sequences of lessons.

Online Safety – Long Term Overview Links with RSHE and ICT coverage			
	Autumn	Spring	Summer
Robins			
RSHE	Theme: All About me	Theme: Feelings	Theme: Good Health
	• How technology makes you feel • Device free moments • Rings of responsibility • Finding my media balance	• Media balance importance • This is me - my identity, thoughts and feelings • Free to be me – who am I? • Beyond gender stereotypes	• Pause and think • Who is in your online community? • Digital citizenship • Grooming • County Lines guidance • Childnet – trust me
ICT	Theme: Media balance & wellbeing	Theme: My Digital Footprint & Identity	Theme: Relationships & Communication
	• My media choices • Digital passport • Staying safe online	• Pause and think online • Digital trails • Online tracks	• Keeping games fun, safe and healthy • Digital friendships
Falcons			
RSHE	Theme: Keeping myself safe	Theme: Growing & changing	Theme: The World Around Me
	• Media balance • Putting a stop to online meanness • Getting help • Being internet secure and kind / responsibility for own behaviour • Grooming	• Safety in my online neighbourhood • Internet traffic lights • That's private! • Who's safe and how do I know?	• Pause for people • Let's give credit! • Is seeing believing? • How long do things stay online? • Things spread quickly • Media vs reality
ICT	Theme – Cyberbullying	Theme – Personal Privacy and Security	Theme – News and Media Literacy
	• Digital citizens • Is it cyberbullying? • Pause and think online • Net aware – networks, apps and games	• Password powerup • Private and personal information • Website cookies • Sharing information	• Rights and responsibilities • News online – fact and fake news – /AI and deep fake • Where are your photos going?

Eagles and Kestrels			
RSHE	Theme: Self-Awareness	Theme: Managing Feelings	Theme: Healthy lifestyles
	• Making responsible choices • Online interactions • Who am I talking to? • Content and contact – evaluating representations online • Internet traffic light • Online issues – key themes • Media pressures and influences online • How social media can affect me	• Forms of communication – gifs, emojis, memes • Safe behaviours online • Trust and is it truth? • Chat rooms and groups • Sharing online and consequences • Respect and consent – boundaries • Online connections and contacts – who can I trust? • Grooming/cat fishing	• Impact of technology on health and wellbeing – positive and negative – how to manage • Tips and advice to promote healthy online use • Accessing health and wellbeing advice online • Pressures that technology place on people and how to manage this • Consent/ Peer Pressure • Persuasive design and content
ICT	Theme: self-image and identity	Theme – Online relationships	Theme: health, wellbeing and lifestyle
	ICT Themes: Media Balance/Wellbeing/ Cyberbullying • My identity online and offline • Copying, modifying and altering identity • How and where to get help on and offline	ICT Themes: My Digital Footprint/ Identity/ Personal Privacy and Security • Online communities • Positive online contributions • How to identify and support myself and others online – • Accessing age appropriate material	ICT Themes: Relationships/ Communication/ News and Media Literacy • Permission and consent • Age restrictions and regulations – content and purpose • Payments for apps and games – consent • On line gambling

Red Kites			
RSHE	Theme: Self-Care, Support and Safety	Theme: Changing and Growing	Theme - The World I live in
	- How to capture bullying content as evidence -what does it look like? - Perception and viewpoint – making accurate judgements - How to help people - Healthy and unhealthy relationship behaviour - Positive online reputation - Influences online - Managing pressure - Live streaming	- Sharing details - Identifying and recognising being targeted by groups/apps and what to do - Sharing information and images/ nudes and sextortion - Permission and consent - Free apps and services - Gambling online - Grooming Harassment online	- Being sceptical - Evaluating digital content - Making safe choices - Key concepts- fact, opinion, belief, evidence and reliability - Being drawn into an agenda or targeted - Impact of media and its influence on my opinions - Addressing extremism and radicalisation - Online influencer - Body image/ Impact of social media
ICT	Theme: Online bullying and reputation	Theme: Privacy and Security	Theme: managing online information, copyright and ownership
	- ICT Themes: Media Balance/Wellbeing/ Cyberbullying - How to block abusive users - How to recognise and report online bullying - Protecting my digital personality - Degrees of anonymity - Helpline services	- ICT Themes: My Digital Footprint/ Identity/ Personal Privacy and Security - Managing passwords, privacy settings and information - How to increase privacy and security settings - Lost and stolen ID - Using Bank apps safely/ scams - Ways to pay/ safe spending	- ICT Themes: Relationships/ Communication/ News and Media Literacy - Search technologies and engines - Evaluating digital content - When it's acceptable to use the work of others/ AI and the law - Permitted content / images

Whilst following this sequence of lessons, pupils in Secondary will complete online learning courses and assessments that bring together the learning and progress to achieve certificates of completion and recognised qualifications.

Certificates of completion – EVERFI learning platform:

The Compassion Project: Kindness in the Classroom	Introduces what it means to be kind to yourself and others, offering a simple framework for empathy and compassion: See, Care, Do. It takes pupils through what compassion looks and sounds like in easily relatable classroom and playtime situations. Pupils also look at the basics of mindful breathing and how it can help them to manage their feelings.
The Compassion Project: Positive Relationships	Explores the complexity of our emotions and how empathy and compassion can help us to build positive relationships. Pupils explore growth mindset and how to compassionately handle mistakes made by themselves and others. Finally, pupils learn about self-care and discover various techniques to help manage intense emotions.
Ignition: Digital Wellness & Safety	Pupils learn about modern digital health concepts such as digital emotional intelligence, digital dependency, online privacy, and evaluating content for accuracy & perspective.
Understanding Mental Wellbeing	Teaches pupils the importance of paying attention to their mental health by blending evidence-informed content with engaging digital activities. Five lessons scaffold knowledge to build a comprehensive understanding of what mental well-being is and how to maintain or achieve it.



Grange Academy Acceptable Use Procedure

Information technology (IT), including email, the internet, and mobile devices are an expected part of our daily working life in school. This procedure is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. It serves to protect staff, visitors, and pupils from harm on the internet, safeguard the school from inappropriate use of the internet, and put in place a procedure to follow in the event of unacceptable use of the school's IT equipment.

All staff are expected to sign and adhere to this procedure at all times. Any concerns or desire for clarification should be raised with the designated or deputy safeguarding lead, or the headteacher.

1. I will ensure my logon details are not shared or used by students or other staff members under any circumstances.
2. When away from my desk I will ensure I am logged out or that my display screen is locked.
3. The school IT systems may not be used for private purposes, unless the headteacher has given permission for that use.
4. I will ensure that all electronic communications with pupils and staff is professional and appropriate.
5. Staff personal details, such as mobile phone numbers or personal email addresses, must never be disclosed to pupils.
6. I will only use the school email system for school business and not for personal use.
7. I will ensure that personal data (defined as any combination of data items that identifies an individual and provides specific information about them, their families, or circumstances) is kept secure and is used appropriately, whether in school, taken off the school premises, or accessed remotely. Electronic personal data can only be taken out of school on an encrypted memory stick.
8. The installation of any third party software applications on school IT equipment must first be authorised by the IT technician.
9. I understand that it is my right to communicate with pupils' parents and carers whom I have a friendship with, through social networking sites, apps, etc. However, discussion of specific Grange Academy matters should not occur, while a positive general image of the school conveyed.
10. I will not intentionally browse, download, upload or distribute any material that is likely to be considered offensive, illegal or discriminatory.
11. Images of pupils will only be taken, stored and used for professional purposes in line with school policy and with written consent of the child's parent or carer. Images will not be shared outside the school network without the permission of the parent/carers.
12. I will not use social networking sites, apps, etc. to either post/discuss issues relating to Grange Academy.
13. Mobile phones are not permitted to be used on the school site unless authorised by the headteacher, by colleagues on their breaks, or for very occasional use by office staff or teachers' on PPA. This policy allows us to model the behaviour we expect from pupils. The school appreciates the enhanced communication that use of mobile phones provides when supporting pupils during educational visits. It is wholly reasonable for staff to use their own phones for personal use during their 'down time' on residential trips.

14. The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is, or may have, taken place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
15. I will not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community. There may be some occasions when sharing potential offensive content, such as swastika, appropriately can lead to good learning outcomes. Should there be any doubt, staff should be duly cautious and discuss the use of potentially offensive content with their line manager before it is browsed, downloaded, uploaded or distributed.
16. It is not the school's policy, as a matter of routine, to monitor an employee's use of the academy's email service, or of the internet, via the school's network. However, when there is reasonable grounds to suspect an instance of misuse of any of these services, the headteacher or Local Advisory Board (LAB) may grant permission for the auditing of an employee's email or their internet use. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the headteacher. These staff are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the headteacher, LAB, or their delegated representative to enable Human Resources to advise the appropriate line manager of the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.
17. I will ensure that my online activity, both in school and outside school, will not bring my professional role, or Grange Academy, into disrepute.
18. I will not correspond with current or present pupils on social networking sites, apps, etc. Existing contact with alumni must be shared with the headteacher and a suitable solution agreed. It maybe that the contact is recorded and approved.
19. I will support and promote the school's e-safety policy and help pupils to be safe and responsible in their use of IT and related technologies.
20. E-mails should be written carefully and politely, to ensure the reader's interpretations are as intended by the writer, particularly as messages may be forwarded or printed and be seen by unexpected readers. Potentially challenging discussions as best conducted face-to-face.

I agree to follow this procedure and to support the safe use of IT throughout the school.

Signed:	
Name:	
Job Title:	
Date:	