



# Knightsfield School

## Online Safety Policy November 2024

Date policy last reviewed: November 2024

Signed by:

Headteacher

Date:

---

---

Chair of Trustees

Date:

---

---

## Contents:

### Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Use of Artificial Intelligence \(AI\)](#)
15. [Educating parents](#)
16. [Internet access](#)
17. [Filtering and monitoring online activity](#)
18. [Network security](#)
19. [Emails](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Links with other policies](#)
25. [Monitoring and review](#)

### **Appendices**

- A. [Online harms and risks – curriculum coverage](#)
- B. [Online Safety Acceptable Use Agreement – Staff and Trustees](#)

## Statement of intent

Knightsfield school understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff. The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

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

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

## Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

## Roles and responsibilities

The trustee board is responsible for:

- The trustee board has overall responsibility for monitoring this policy and holding the acting-headteacher to account for its implementation.
- The trustee board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The trustee board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The trustee board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The trustee board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The trustee board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
  - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
  - Reviewing filtering and monitoring provisions at least annually;
  - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
  - Having effective monitoring strategies in place that meet their safeguarding needs.
- The trustee who oversees online safety is **Robert Marshall**
- All trustees will:
  - Ensure they have read and understand this policy
  - Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix B)
  - Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures.

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The acting-headteacher is responsible for:

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

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.  
Working closely with the police during police investigations.
- Keeping up-to-date with current research, legislation and online trends.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Working with the acting-headteacher and trustee board to update this policy on an **annual** basis.

The Deputy DSL/Deputy headteacher is responsible for:

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day
- **ICT across the curriculum.**

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the acting-headteacher.

- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems to the DSL
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Ensuring any instance of cyber-bullying is reported so it can be dealt with appropriately in line with the behaviour policy.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

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

Parents are expected to:

- Notify the acting-headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on the acceptable use of the school's ICT systems and internet agreement.

## Managing online safety

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

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the acting-headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

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

- Online safety discrete lessons
- Half-termly online safety newsletters (provided by HertsforLearning)
- Staff and trustees receive regular training (at least annually)
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online

## Handling online safety concerns

- Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.
- Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not

being reported, does not mean it is not happening.

- Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.
- The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.
- Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.
- Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.
- Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the acting-headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.
- Where there is a concern that illegal activity has taken place, the acting-headteacher contacts the police.
- The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.
- All online safety incidents and the school's response are recorded by the DSL.

## **Cyberbullying**

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

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

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

## **Child-on-child sexual abuse and harassment**

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

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

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse
- All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.
- Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

Knightsfield school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse **guidance (within the Child Protection policy)** and the Social Media Policy.

Knightsfield school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

## Grooming and exploitation

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

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

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

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.



- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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

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

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

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

### **Radicalisation**

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

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

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty **guidance within the Child Protection policy**.

## **Mental health**

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

Staff at Knightsfield school will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

## **Online hoaxes and harmful online challenges**

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

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

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

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

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

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The DSL and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

## Cyber-crime

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

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

Knightsfield school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the appropriate body.

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

## Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

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

## Online safety and the curriculum

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

- RSE

- Careers
- PSHE and Citizenship
- iDEA ICT curriculum

At Knightsfield school, online safety teaching is always appropriate to pupils' ages and developmental stages. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [appendix A](#) of this policy.

The **Deputy Headteacher/DDSL** is **responsible for** the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

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

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

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

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

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The acting-headteacher and **Deputy headteacher/DDSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and **Deputy Headteacher/DDSL** consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The **Deputy headteacher/DDSL** advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

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

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member

will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

## Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Google phones (Year 5/6 only)
- Internet
- Email
- Cameras
- iPads

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

## Use of smart technology

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

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

Staff will use all smart technology and personal technology in line with the school's **Mobile Phone policy and ICT Acceptable Use Agreement.**

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

Inappropriate use of smart technology may include:

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

Pupils will not be permitted to use smart devices or any other personal technology **at any time during the school day.**

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

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

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

## Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Knightsfield School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Knightsfield will treat any use of AI to bully pupils in line with our cyber bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by Knightsfield School.

## Educating parents

Knightsfield school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are sent a copy of the Acceptable Use Agreement at **the beginning of each academic year** and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

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

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

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

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

- Parents' evenings
- Twilight training sessions
- Weekly newsletters
- Online resources

## Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

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

## Filtering and monitoring online activity

The trustee board of Knightsfield school ensures the school's ICT network has appropriate filters and monitoring systems in place. The trustee board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The school uses Herts for Learning to provide filtering and monitoring systems appropriate to pupils' ages. The ICT technician conducts a weekly check on the filtering and monitoring systems to ensure they are effective and appropriate. This report is submitted to the DSL each week who discusses at the fortnightly DSP meeting. In addition, members of SLT receive reports from Senso which alert them to 'live' potential breaches.

Requests regarding making changes to the filtering system are directed to the acting-headteacher.

Deliberate breaches of the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Child Protection and Safeguarding Policy.

## Network security

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

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to SLT.

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

Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

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

## Emails

Access to and the use of emails at Knightsfield school is managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. The school email is multi-authenticated. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Online safety lessons and workshops have explained what a phishing email and other malicious emails may look like and includes information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

## Social networking

### Personal use

At Knightsfield school access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct and the Social media policy contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and acting-headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

### Use on behalf of the school

Knightsfield school's official social media channels are only used for official educational or engagement purposes. Staff



members must be authorised by the acting-headteacher to access to the school's social media accounts. All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

## **The school website**

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

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the appropriate permissions are met.

## **Use of devices**

### **School-owned devices**

Some Knightsfield school staff members are issued with the following devices to assist with their work. The ICT technician is responsible for keeping a record of who is issued with a lap-top and ensuring an agreement is signed:

- Laptop

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

ICT technicians review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

### **Personal devices**

Personal devices are not permitted to be used in **the school at all, but most particularly not in the** following locations:

- Toilets
- Changing rooms

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members report concerns about their colleagues' use of personal devices on the school premises. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the acting-headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

**Pupils are not permitted to use their personal devices at any time during the school day.** If a pupil needs to contact their parents during the school day, they are allowed to use the phone in **the school office**. The acting-headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Where a pupil uses accessibility features on a personal device to help them access education, e.g. where our deaf pupils use their mobile phone to adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

**The exception to this is with Post-16 students. The school has purchased notetaking software to streamline the support at college and in the 6<sup>th</sup> form. The software is called Jamworks and students have their own log in to the software. They are able to use their devices to record the lessons they attend with the software then generating summaries, quizzes and resources based upon the lesson. This has been agreed with Oaklands College and Monk's Walk School. The software also encourages independence as the student will not need 1:1 support in every lesson from a member of staff.**

Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

## Remote learning

Knightsfield school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

If there is a period of remote learning, Knightsfield school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

## Links with other policies

The Online Safety policy is linked to our:

- Child Protection and Safeguarding policies
- Behaviour Policy
- Staff Disciplinary Procedure
- Data Protection Policy and associated notices
- Complaints Procedure
- **Mobile Phone Policy**
- Social Media Policy
- ICT and internet acceptable use agreements

## Monitoring and review

Knightsfield school recognises that the online world is constantly changing; therefore, the DSL, Deputy headteacher and the acting-headteacher conduct reviews of this policy to evaluate its effectiveness throughout the year.

The trustee board, acting-headteacher and DSL review this policy in full on an **annual** basis and following any online safety incidents.

The next scheduled review date for this policy is **October 2025**

Any changes made to this policy are communicated to all members of the school community

Appendix A

## Online harms and risks – curriculum coverage



Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
<b>How to navigate the internet and manage information</b>		
Age restrictions	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That age verification exists and why some online platforms ask users to verify their age</li> <li>• Why age restrictions exist</li> <li>• That content that requires age verification can be damaging to under-age consumers</li> <li>• What the age of digital consent is (13 for most platforms) and why it is important</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHCE</li> <li>• Online Safety/iDEA Lessons</li> <li>• PSHCE</li> <li>• Behaviour curriculum</li> </ul>
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What a digital footprint is, how it develops and how it can affect pupils' futures</li> <li>• How cookies work</li> <li>• How content can be shared, tagged and traced</li> <li>• How difficult it is to remove something once it has been shared online</li> <li>• What is illegal online, e.g. youth-produced sexual imagery (sexting)</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE/Citizenship</li> </ul>
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• Disinformation and why individuals or groups choose to share false information in order to deliberately deceive</li> <li>• Misinformation and being aware that false and misleading information can be shared inadvertently</li> <li>• Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons</li> <li>• That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online</li> <li>• How to measure and check authenticity online</li> <li>• The potential consequences of sharing information that may not be true</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships and health education</li> <li>• PSHCE/Online safety/iDEA</li> <li>• PSHCE/Citizenship</li> </ul>

Fake websites and scam emails	<p>Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How to recognise fake URLs and websites</li> <li>• What secure markings on websites are and how to assess the sources of emails</li> <li>• The risks of entering information to a website which is not secure</li> <li>• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email</li> <li>• Who pupils should go to for support</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> </ul>
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What identity fraud, scams and phishing are</li> <li>• That children are sometimes targeted to access adults' data</li> <li>• What 'good' companies will and will not do when it comes to personal details</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> <li>• Maths</li> </ul>
Password phishing	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• Why passwords are important, how to keep them safe and that others might try to get people to reveal them</li> <li>• How to recognise phishing scams</li> <li>• The importance of online security to protect against viruses that are designed to gain access to password information</li> <li>• What to do when a password is compromised or thought to be compromised</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> </ul>
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How cookies work</li> <li>• How data is farmed from sources which look neutral</li> <li>• How and why personal data is shared by online companies</li> <li>• How pupils can protect themselves and that acting quickly is essential when something happens</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• iDEA</li> </ul>

	<ul style="list-style-type: none"> <li>• The rights children have with regards to their data</li> <li>• How to limit the data companies can gather</li> </ul>	<ul style="list-style-type: none"> <li>• Careers</li> </ul>
Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible</li> <li>• How notifications are used to pull users back online</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• iDEA/Online Safety</li> <li>• PSHCE</li> <li>• Citizenship</li> </ul>
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How to find information about privacy settings on various devices and platforms</li> <li>• That privacy settings have limitations</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> <li>• Behaviour curriculum</li> </ul>
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts</li> <li>• How the targeting is done</li> <li>• The concept of clickbait and how companies can use it to draw people to their sites and services</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• English</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> <li>• Careers</li> </ul>
How to stay safe online		

Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• The types of online abuse, including sexual harassment, bullying, trolling and intimidation</li> <li>• When online abuse can become illegal</li> <li>• How to respond to online abuse and how to access support</li> <li>• How to respond when the abuse is anonymous</li> <li>• The potential implications of online abuse</li> <li>• What acceptable and unacceptable online behaviours look like</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> <li>• Behaviour curriculum</li> <li>• Citizenship</li> </ul>
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal</li> <li>• How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why</li> <li>• That it is okay to say no and to not take part in a challenge</li> <li>• How and where to go for help</li> <li>• The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Behaviour curriculum</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> </ul>
Content which incites violence	<p>Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That online content (sometimes gang related) can glamorise the possession of weapons and drugs</li> <li>• That to intentionally encourage or assist in an offence is also a criminal offence</li> <li>• How and where to get help if they are worried about involvement in violence</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Idea/Online Safety</li> <li>• PSHCE</li> <li>• Citizenship</li> </ul>
Fake profiles	<p>Not everyone online is who they say they are. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That, in some cases, profiles may be people posing as someone they are not or may be 'bots'</li> <li>• How to look out for fake profiles</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> </ul>

		<ul style="list-style-type: none"> <li>• Behaviour curriculum</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> <li>• Citizenship</li> </ul>
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• Boundaries in friendships with peers, in families, and with others</li> <li>• Key indicators of grooming behaviour</li> <li>• The importance of disengaging from contact with suspected grooming and telling a trusted adult</li> <li>• How and where to report grooming both in school and to the police</li> </ul> <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• Behaviour curriculum</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> </ul>
Livestreaming	<p>Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content</li> <li>• The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely</li> <li>• That online behaviours should mirror offline behaviours and that this should be considered when making a livestream</li> <li>• That pupils should not feel pressured to do something online that they would not do offline</li> <li>• Why people sometimes do and say things online that they would never consider appropriate offline</li> <li>• The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next</li> <li>• The risks of grooming</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> </ul>
Pornography	<p>Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following:</p>	<p>This risk or harm is covered in the</p>

	<ul style="list-style-type: none"> <li>• That pornography is not an accurate portrayal of adult sexual relationships</li> <li>• That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour</li> <li>• That not all people featured in pornographic material are doing so willingly, i.e. revenge porn or people trafficked into sex work</li> </ul>	<p>following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHCE</li> <li>• Idea/Online Safety</li> </ul>
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with</li> <li>• How to identify indicators of risk and unsafe communications</li> <li>• The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before</li> <li>• What online consent is and how to develop strategies to confidently say no to both friends and strangers online</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• Behaviour curriculum</li> <li>• PSHCE</li> <li>• Idea/Online Safety</li> <li>• English</li> </ul>
<b>Wellbeing</b>		
Impact on confidence (including body confidence)	<p>Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• The issue of using image filters and digital enhancement</li> <li>• The role of social media influencers, including that they are paid to influence the behaviour of their followers</li> <li>• The issue of photo manipulation, including why people do it and how to look out for it</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHCE</li> <li>• Science</li> <li>• iDEA</li> </ul>
Impact on quality of life, physical and mental health and relationships	<p>Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)</li> <li>• How to consider quality vs. quantity of online activity</li> <li>• The need for pupils to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out</li> <li>• That time spent online gives users less time to do other activities, which can lead some users to become physically inactive</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• iDEA/online safety</li> <li>• PSHCE</li> </ul>

	<ul style="list-style-type: none"> <li>• The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues</li> <li>• That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support</li> <li>• Where to get help</li> </ul>	
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives</li> <li>• How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• Relationships education</li> <li>• PSHCE</li> <li>• iDEA</li> </ul>
Reputational damage	<p>What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following:</p> <ul style="list-style-type: none"> <li>• Strategies for positive use</li> <li>• How to build a professional online profile</li> </ul>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHCE</li> <li>• Careers</li> <li>• English</li> <li>• iDEA</li> </ul>
Suicide, self-harm and eating disorders	<p>Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	<p>This risk or harm is covered in the following curriculum areas:</p> <ul style="list-style-type: none"> <li>• PSHCE</li> <li>• Idea/Online Safety</li> <li>• science</li> </ul>

## **Online Safety Acceptable Use Agreement - Staff, Trustees and student teachers (on placement or on staff)**

You must read this agreement in conjunction with the online safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and trustees are aware of their responsibilities in relation to their use. All staff, student teachers and trustees are expected to adhere to this agreement and to the online safety policy. Any concerns or clarification should be discussed with Danny Bidwell. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

### **Internet Access**

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on Knightsfield School equipment must be treated as an online safety incident, reported to the online safety lead and/or DSP and an incident report completed.

### **Online conduct**

I will ensure that my online activity, both in and outside school, will not bring Knightsfield School, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to Danny Bidwell.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to pupils and/or parents/carers.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, Trustees, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

### **Passwords**

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.



## **Data protection**

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or trustee board
- Personal or sensitive data taken off site must never be taken offsite unless with the express permission of the Headteacher. The school has provided all staff with secure access to the Knightsfield network via LARA (remote access).

## **Images and videos**

I will only upload images or videos of staff, pupils or parents/carers onto Knightsfield School approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of Knightsfield School events or activities on any personal device.

## **Use of email**

I will use my Knightsfield School email address or Trustee hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses for personal matters or non-school business.

## **Use of personal devices**

I understand that as a member of staff I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in Knightsfield School is at the discretion of the headteacher.

I will only use approved personal devices in designated areas (the staff room) and never in front of pupils.

I will only access secure Knightsfield School information from personal devices through the OneDrive service, Edulink or Office 365 when in school or any other location. Such a system would ensure as the user I was not saving files locally to my own device and breaching data security

A 'monitorable system' would be one such as One Drive. Through One Drive, any school documents accessed on a personal device are never actually on the computer being used, they remain on the school server. When the user logs-out of One Drive, there are no copies left on their own device.

## **Additional hardware/software**

I will not install any hardware or software on Knightsfield School equipment without permission of Danny Bidwell.

## **Promoting online safety**

I understand that online safety is the responsibility of all staff and Trustees and I will promote positive online safety

messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, Trustees, visitors, pupils or parents/carers) to the DSP or Danny Bidwell

### **Classroom management of internet access**

I will pre-check for appropriateness all internet sites used in the classroom this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of pupils. I will also check the appropriacy of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with Danny Bidwell

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the Knightsfield School Senior Leadership Team and DSP. A school-owned device should be used when running video-conferences, where possible.

### **User signature**

I agree to follow this Acceptable Use Agreement and to support online safety throughout the Knightsfield School. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a trustee.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....