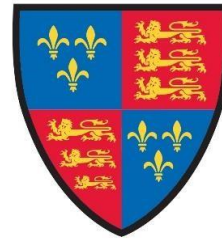




**THE SCHOOLS OF  
KING EDWARD VI  
IN BIRMINGHAM**



*In pursuit of educational excellence for all*



**KING EDWARD VI  
ACADEMY TRUST  
BIRMINGHAM**

## Online Safety Policy

<b>Responsible Board/Committee</b>	Academy Trust Board Foundation Board
<b>Policy Type</b>	Hybrid Policy
<b>Policy Owner</b>	Education and Digital Transformation
<b>Statutory</b>	Yes
<b>Publish Online</b>	Yes
<b>Last Review Date</b>	September 2023
<b>Review Cycle</b>	Annual
<b>Next Review Date</b>	August 2024
<b>Expiry Date</b>	October 2024
<b>Version</b>	2.1

<b>School</b>	King Edward VI Northfield School for Girls
<b>School Policy Owner</b>	Luke Atkinson
<b>LGB Approval Date</b>	

## 1. Introduction

The Foundation aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers the Foundation to protect and educate the whole school community in its conduct and use of all technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 2. Legislation and Guidance

### 2.1 Legislation

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [teaching online safety in schools](#)
- [preventing and tackling bullying](#)
- [searching, screening and confiscation](#).
- [Cyber security standards](#)

It also refers to the Department's guidance on [protecting children from radicalisation: the Prevent Duty](#). It 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. It also takes into account guidelines detailed in the Department's [filtering and monitoring standards](#).

### 2.2 Protecting Personal Data

The Foundation believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. Schools collect personal data from pupils, parents / carers, and staff and process it in order to support teaching and learning; monitor and report on pupil and teacher progress; and strengthen pastoral and safeguarding provision.

The Foundation takes responsibility for ensuring that any data that is collected and processed is used correctly and only as is necessary. Parents / carers will be kept fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that is needed. Through effective data management a range of school provisions, including the wellbeing and academic progression of our pupils, can be monitored and evaluated to ensure that they are being fully supported.

In line with the United Kingdom General Data Protection Regulation ('UK GDPR') and Data Protection Act 2018, and following principles of good practice when processing data, the Foundation will:

- Ensure that data is fairly and lawfully processed;
- Process data only for limited purposes;
- Ensure that all data processed is adequate, relevant and not excessive;
- Ensure that data processed is accurate;
- Not keep data longer than is necessary;
- Process the data in accordance with the data subject's rights;
- Ensure that data is secure;
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where schools are required either by law or in the best interests of pupils or staff to pass information onto external authorities, for example, the local authority, Ofsted, or the Department of Health. These authorities comply with data protection law and have their own policies relating to the protection of any data that they receive or collect.

While complying with data protection legislation is important and will always be considered, the safeguarding of students is our main priority – concerns around data protection should not prevent a safeguarding disclosure being investigated.

### **3. Roles and responsibilities**

#### **3.1 The Trustee Board and Local Governing Body**

The Trustee Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, our governing body will do all that it reasonably can to limit children's exposure online safety risks. As part of this process, they will ensure our schools has appropriate filtering and monitoring systems in place and will regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Our governing body will consider the number of and age range of our pupils, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

The Local Governing Body will co-ordinate regular meetings with appropriate staff to review online safety incidents and safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's technology and digital systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

### 3.2 The Headteacher

The Headteacher has a duty of care for ensuring the safety (including digital safety) of members of the school community, and is therefore responsible for:

- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- ensuring that the relevant staff receive suitable training to enable them to carry out their digital safety roles
- Being aware of the procedures to be followed in the event of a serious digital safety allegation being made against a member of staff.
- Ensuring appropriate action is taken in all cases of misuse

The Education and Inspections Act 2006 grants the Headteacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

### 3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and any deputies are set out in each school's child protection and safeguarding policy.

The DSL should be appropriately trained in digital safety issues (including understanding the filtering and monitoring systems and processes in place).

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Being aware of the potential for serious child protection / safeguarding issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate digital contact with strangers, incidents of grooming and cyberbullying
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety and preventative digital safeguarding measures.
- Liaising with other agencies and / or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Local Governing Body
- Providing regular updates for parents / carers and opportunities for them to engage in training on digital safety
- Ensuring that there are appropriate processes and systems in place for protecting pupils online, e.g., filtering and monitoring

This list is not intended to be exhaustive.

### 3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. Details of the current filtering and monitoring in use are available on request
- To provide DSL with filtering and monitoring report.
- Ensuring that the school's technology and digital systems are secure and protected against viruses and malware, and that such safety mechanisms are updated and checked regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files, without unreasonably impacting teaching and learning.
- Ensuring that staff do not have the option to install on school devices any software that is not on the 'allowed' list
- Ensuring that school devices are protected using suitably secure passwords and multi-factor authentication system

This list is not intended to be exhaustive.

### 3.5 The School Community

Pupils, staff and parents / carers are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The Foundation expects all staff, pupils and parents / carers to remember that they are representing the Schools of King Edward VI community at all times and must act appropriately.

Cyber Bullying is viewed in the same light as any other form of bullying and we will follow the same procedures and sanctions. Sanctions will be issued by the school in line with the severity of the incident and may be internal or external suspensions or permanent exclusion in the most serious cases.

### 3.6 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers have a duty of care and are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged on MyConcern.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately to all reports and concerns about sexual violence and / or harassment, both online and offline and maintaining an attitude of 'it does happen here'
- Ensuring they only use official school-provided email accounts to communicate with pupils, parents / carers and that any communication should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
- Informing their Line Manager or a member of the Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves. Further advice can be sought through The Professionals Online Safety Helpline (POSH) on 0344 381 4772 or via [helpline@saferrinternet.org.uk](mailto:helpline@saferrinternet.org.uk)

This list is not intended to be exhaustive.

All staff, governors and volunteers should receive appropriate online safety training which amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Teachers must also consider their own digital footprint and ensure they adhere to the Teacher Standards.

### 3.7 Parents/ Carers

Outside school, parents / carers bear the same responsibility for guidance as they would normally exercise with information sources such as television, telephones, films, radio and other media.

Appropriate home use of the Internet by children can be educationally beneficial, and can make a useful contribution to home and school work. It should, however, be supervised, and parents / carers should be aware that they are responsible for their children's use of Internet resources at home. In addition, if there is a period of school closure which necessitates the wider use of video / audio conferencing to supplement or deliver teaching and learning, the principles of this policy and usual sanctions will apply.

Parents / carers are expected to:

- Notify a member of staff of any concerns or queries regarding this policy or online safety. Please call reception 0121 4648346 and report any online incident to the relevant Head of Year or member of safeguarding team.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

### 4.8 Visitors and members of the community

Visitors and members of the community who use the school's technology and digital 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 terms on acceptable use.

## 4. Educating Pupils about online safety

It is essential that our pupils are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school to protect and

educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

- content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- contact: being subjected to harmful online interaction with other users; for example: child-on-child abuse, 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; for example, 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. If you feel your pupils, pupils or staff are at risk, please report it to the [Anti-Phishing Working Group](#).

All secondary schools have to teach [Relationships and Sex Education and Health Education](#).

Pupils will be taught about online safety as part of the curriculum and school assembly programme.

In Key Stage 3, pupils will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

Not to provide material to others that they would not want shared further and not to share personal material which is sent to them

What to do and where to get support to report material or manage issues online

The impact of viewing harmful content

That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail

How information and data is generated, collected, shared and used online

How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## **5. Educating Parents/ Carers about online safety**

Parents and carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Every opportunity will be taken to help parents / carers understand these issues. The school will raise parents' / carers' awareness of internet safety in letters or other communications home, and in information via the school website.

These letters and communications enable school to keep parents/ carers informed and updated regarding the school online filtering and monitoring systems, in addition to outlining our expectations on online tasks, websites and school contacts for pupils.

Online safety will also be covered during parents' / carers' evenings.

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

- What are the issues? [UK Safer Internet Centre](#)
- Hot topics, [Childnet International](#)
- Parent / carer factsheet, [Childnet International](#)
- Healthy relationships: [Disrespect Nobody](#)
- Report a concern to CEOP that a child is being groomed online or sexually exploited <http://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/>

## **6. Cyber-Bullying**

### **6.1 Definition**

Cyber-bullying takes place online, such as through social networking sites, messaging apps, chatrooms or gaming sites such as Snapchat, Twitter or TikTok and involves the harassment, threat, embarrassment, intimidation or targeting of someone. 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 school behaviour policy.) Unlike



physical bullying, cyber-bullying can often be difficult to track as the cyber-bully (the person responsible for the acts of cyber-bullying) can remain anonymous when threatening others online, encouraging them to behave more aggressively than they might face-to-face.

## 6.2 Preventing and addressing cyber-bullying

All our pupils understand our school's approach and are clear about the part they can play to prevent cyber-bullying, including when they should be upstanders not bystanders.

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. In line with our safeguarding policy, procedures and training, pupils are supported by staff to report cyber-bullying, including where they are a witness rather than the victim, so that they are assured that they will be listened to and incidents acted on.

We do our best to create an inclusive atmosphere in school by encouraging open discussions about the differences between people that could motivate any form of bullying, such as religion; ethnicity; disability; gender; sexuality; appearance related difference; different family situations, children being in the care system; or those with caring responsibilities. We also teach our pupils that using any prejudice-based language is unacceptable.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs and the forms it may take. Pupils also know that the school will implement disciplinary sanctions which will reflect the seriousness of the incident so that others see that cyber-bullying is unacceptable and that their behaviour is wrong.

Class teachers/form teachers will discuss cyber-bullying with their tutor groups, 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 school also sends information / leaflets on cyber-bullying to parents / carers 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 school 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.

## 6.3 Examining electronic devices

School 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. These powers are compatible with Article 8 of the European Convention on Human Rights.

DfE guidance states that parental / carer consent is not required to search through a young person's mobile phone. If a member of staff has reasonable grounds to suspect the device provides evidence that an individual has committed an offence, it should be retained and passed to the police.

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:

- Cause harm, and/or
- Disrupt teaching, and/or
- 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:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police (staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.)

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#) and UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

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

## **7. Acceptable Use of the Internet in school**

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

All pupils, parents / carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of school owned and managed hardware, such as computers, to access the 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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

## **8. Pupils using mobile devices in school**

The King Edward VI Foundation expects all schools to have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited

and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means whilst at school, child-on-child abuse, bullying or sexually harassment via mobile and smart technology, sharing of indecent images consensually and non-consensually (often via online chat groups) and viewing and sharing pornography and other harmful content may occur. Our schools should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection and safeguarding policy.

Any pupil who brings a mobile phone or personal device into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen or damaged.

If pupils choose to bring mobile phones to school, they should be switched off and kept away in bags or blazers. Mobile phones should not be seen in school and pupils can expect them to be confiscated and a detention issued if they have them out in school.

### **9. Staff using school owned and managed devices outside school**

Staff members using a work device outside school must not use the device in any way which would violate the school's terms of acceptable use, as set out in [appendix 2.]

Staff must ensure 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 school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. If they receive inappropriate contact or content, including threats or defamation, they should report to their Line Manager immediately.

Work devices must be used solely for work activities.

## **10. How the school will respond to issues of misuse**

### **10.1 Misuse**

Where a pupil misuses the school's technology and digital systems or internet, we will discuss the incident with pupil and parent if required. 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 school's technology and digital 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 school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and, making, supplying or obtaining malware (malicious software) such as viruses, spyware ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online and child sexual abuse and exploitation, nor other areas of concern such as online bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK

## 10.2 Procedures for staff if they are being cyber bullied

Staff should never respond or retaliate to cyberbullying incidents. They should report incidents appropriately and seek support from a line manager or a senior member of staff. Evidence of the abuse such as screen shots of messages or web pages should be saved, together with a record of the time and date.

Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures. Where the perpetrator is known to be an adult, a meeting will be held with the victim to address concerns, and appropriate measures will be taken, including ensuring the offending comments are removed.

Schools or individuals can report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre [www.saferinternet.org.uk](http://www.saferinternet.org.uk) or [Professional Online Safety Helpline](http://www.professionalsafetyhelpline.co.uk).

If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, individuals or a representative from the school may consider contacting the local police. Online harassment is a crime.

If staff think they have been affected by a hate crime, they can report it [here](#).

## 11.Training

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

All staff should be aware of the systems in their school or college which support safeguarding, and these should be explained to them as part of staff induction. As a minimum the KCSIE Part One and the safeguarding and child protection policy will be shared with staff at induction.

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).

By way of this training, all staff will be made aware that:

- Technology and digital systems is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Child-on-child abuse can occur online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- protect themselves
- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

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

The Headteacher will also undertake child protection and safeguarding training, which will include online safety, at least every two years.

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 child protection and safeguarding policy.

## **12. Monitoring Arrangements**

The DSL logs behaviour and safeguarding issues related to online safety. Safeguarding issues will be logged via MyConcern.

This policy will be reviewed centrally by the Education Department and locally on an annual basis by the DSL. At every review, the policy will be shared with the Local Governing Body.

A review of our filtering and monitoring provision will be completed at least annually.

### **13.Links with other policies**

This online safety policy should be read in conjunction with other policies such as:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints policy
- Staff Code of Conduct

## Appendix 1: ACCEPTABLE USE AGREEMENT (PUPILS AND PARENTS / CARERS)

### ICT and Data Acceptable Use Policy - (September 2023)

#### Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as CDs, flash drives / USBs etc.) with antivirus software. If unsure, get the file checked before loading onto the network.
- Pupil / staff data documents on USBs should be password protected and encrypted.
- Always check mobile equipment (e.g. laptops, tablet PCs, etc.) with antivirus software. If unsure get them checked before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

#### Security and Privacy

- Always lock a school computer when you are not using it, using 'ctrl L' or log off.
- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- If using a home computer for school work, ensure that the home computer has up-to-date virus protection software. Also ensure that if the home computer is shared, users have separate accounts / log-ins. When walking away from your home computer with a document open press 'ctrl L'.
- Hardcopies of pupil or staff data must be kept in a locked cabinet.

#### Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.

#### Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- If emailing pupil / staff information to other agencies / schools always use Egress Switch or password protect and communicate the password separately.

**Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action.** Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_



## Appendix 2: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

### ICT and Data Acceptable Use Policy - Staff Guidelines (September 2023)

#### Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as CDs, flash drives / USBs etc.) with antivirus software. If unsure, get the file checked before loading onto the network.
- Pupil / staff data documents on USBs should be password protected and encrypted.
- Always check mobile equipment (e.g. laptops, tablet PCs, etc.) with antivirus software. If unsure get them checked before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

#### Security and Privacy

- Always lock a school computer when you are not using it, using 'ctrl L' or log off.
- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- If using a home computer for school work, ensure that the home computer has up-to-date virus protection software. Also ensure that if the home computer is shared, users have separate accounts / log-ins. When walking away from your home computer with a document open press 'ctrl L'.
- Hardcopies of pupil or staff data must be kept in a locked cabinet.
- Report data loss to Neil Jones (Data Controller).
- Do not use pupil surnames in displays or on school social media posts / newsletters.

#### Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.

#### Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- If emailing pupil / staff information to other agencies / schools always use Egress Switch or password protect and communicate the password separately.

**Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action.** Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

## Appendix 3: USEFUL LINKS

### Pupils

Children can talk to a ChildLine counsellor 24 hours a day about anything that is worrying them by ringing 0800 1111 or in an online chat at [www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx](http://www.childline.org.uk/Talk/Chat/Pages/OnlineChat.aspx)

[www.childline.org.uk/info-advice/bullying-abuse-safety/digital-mobile-safety/sexting/](http://www.childline.org.uk/info-advice/bullying-abuse-safety/digital-mobile-safety/sexting/) Childline support on sexting.

<https://www.ditchthelabel.org/living-insta-lie/> An amusing reminder about social media v reality.

Zipit – App allowing young people to send humorous responses to anybody who has asked them to send an explicit image.

### Parents / carers

[www.bbc.com/ownit/take-control/own-it-app](http://www.bbc.com/ownit/take-control/own-it-app) The Own It app comes with a special keyboard. This can be used like any other keyboard, but it also gives your child helpful tips and friendly advice as they write.

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/> Whether you're a digital expert or you're not sure where to start, the NSPCC's tools and advice will help you keep your child safe.

[www.saferInternet.org.uk](http://www.saferInternet.org.uk) E-safety tips, advice and resources to help children and young people stay safe digital.

<http://jcoleman.co.uk/wp-content/uploads/2019/01/SocialMedia.pdf> Social media and teenagers. A practical approach. A guide from The Charlie Waller Memorial Trust.

[www.commonsemmedia.org](http://www.commonsemmedia.org) To learn more about the games or apps your children are using, Common Sense Media covers thousands, and includes advice and reviews from other parents / carers.

[www.thinkuknow.co.uk/parents/articles](http://www.thinkuknow.co.uk/parents/articles) Advice and information for parents / carers, including links to report concerns.

[www.Internetmatters.org](http://www.Internetmatters.org) Helping parents / carers keep their children safe digitally.

[www.net-aware.org.uk](http://www.net-aware.org.uk) Online guide to the social networks, sites and apps children use.

[www.childnet.com](http://www.childnet.com) Non-profit organisation working with others to help make the Internet a great and safe place for children.

[www.iwf.org.uk](http://www.iwf.org.uk) Internet Watch Foundation receive, assess and trace public complaints about child sexual abuse content on the internet and support the development of website rating systems. It is also the UK hotline for reporting criminal online content with particular reference to images of child sexual abuse.

<http://parentinfo.org/article/where-do-i-report-if-im-worried-about-my-childs-safety-digital> A parent's / carer's guide to help report digital activity.

[www.parentsprotect.co.uk](http://www.parentsprotect.co.uk) Provides information and resources for parents / carers about child sexual abuse, including a section on online safety.

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/490001/Social\\_Media\\_Guidance\\_UKCCIS\\_Final\\_18122015.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf) Child Safety Digital: A practical guide for parents and carers whose children are using social media.

[www.snapchat.com/l/en-gb/safety/](http://www.snapchat.com/l/en-gb/safety/) and [www.parentinfo.org/article/snapchat-what-to-do-if-you-re-worried](http://www.parentinfo.org/article/snapchat-what-to-do-if-you-re-worried) Snapchat digital safety.

[www.lifewire.com/what-is-instagram-3486316](http://www.lifewire.com/what-is-instagram-3486316) What is Instagram and how is it used?

[www.lifewire.com/what-is-snapchat-3485908](http://www.lifewire.com/what-is-snapchat-3485908) What is Snapchat and how is it used?

[www.connectsafely.org/a-parents-guide-to-mobile-phones](http://www.connectsafely.org/a-parents-guide-to-mobile-phones) A parent's/carer's guide including tips for Smartphone use; helping children protect their safety, privacy and security; and parental controls.

[www.connectsafely.org/wp-content/uploads/A-Parent's-Guide-to-Snapchat.pdf](http://www.connectsafely.org/wp-content/uploads/A-Parent's-Guide-to-Snapchat.pdf) A parent's / carer's guide to Snapchat (US version). Note UK support address on page 5 is:  
<https://support.snapchat.com/en-GB/i-need-help>

<http://www.connectsafely.org/familylink/> This guide provides parents / carers with an overview of the Family Link parental tools with tips on how to set up and manage their child's device, including setting "screen time" to determine how long and at what times they can use their device.

[www.connectsafely.org/fakenews](http://www.connectsafely.org/fakenews) A parent / carer and educator guide to media literacy and fake news.

[www.childrenscommissioner.gov.uk/publication/life-in-likes/](http://www.childrenscommissioner.gov.uk/publication/life-in-likes/) This Children's Commissioner's report on the effects of social media on 8-to-12-year-olds examines the way children use social media and its effects on their wellbeing. 'Life in Likes' fills a gap in research showing how younger children use platforms which social media companies say are not designed for them.

[www.esafety-adviser.com/latest-newsletter/](http://www.esafety-adviser.com/latest-newsletter/) Teachers or parents / carers can sign up to the newsletter which comes out every 6 weeks.

[www.bps.org.uk/news-and-policy/changing-behaviour-children-adolescents-and-screen-use](http://www.bps.org.uk/news-and-policy/changing-behaviour-children-adolescents-and-screen-use) Paper from the British Psychological Society (2018). The recommendations set out in the paper recognise that the issue of children's digital media use is more complex than amount of screen time and acknowledges both benefits and risks to media use.

## **Staff**

Additional guidance on "appropriate" filtering and monitoring can be found at: [UK Safer Internet Centre](http://www.uk-safer-internet-centre.org/)

<https://digital-literacy.org.uk/> South West Grid for Learning provide free materials designed to empower pupils to think critically, behave safely, and participate responsibly in our digital world. Browse by Key Stage or Year Group, for cross-curricular lessons which address digital literacy and citizenship topics in an age-appropriate way.

[www.gov.uk/government/publications/education-for-a-connected-world](http://www.gov.uk/government/publications/education-for-a-connected-world) The Education for a Connected World framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It

highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.

[www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis](http://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) The UK Council for Child Internet Safety is now the UK Council for Internet Safety (UKCIS)

[www.gov.uk/government/publications/teaching-online-safety-in-schools](http://www.gov.uk/government/publications/teaching-online-safety-in-schools) 2019 guidance supporting schools to teach pupils how to stay safe online when studying new and existing subjects.

[www.ofcom.org.uk/\\_data/assets/pdf\\_file/0024/149253/online-nation-summary.pdf](http://www.ofcom.org.uk/_data/assets/pdf_file/0024/149253/online-nation-summary.pdf) - Online Nation is a new annual report that looks at what people are doing online, how they are served by online content providers and platforms, and their attitudes to and experiences of using the internet. It brings the relevant research into a single place and aims to act as a data- and insight driven resource for stakeholders at a time of significant evolution in the online landscape.

[www.e-safetysupport.com/resources/details/?resource\\_type=support\\_advice](http://www.e-safetysupport.com/resources/details/?resource_type=support_advice) What every teacher needs to know about e-safety.

<https://pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2019/02/Vulnerable-Children-in-a-Digital-World-FINAL.pdf> This study looks at a number of vulnerable groups in order to ascertain differences of experiences and vulnerabilities.

[www.rsph.org.uk/our-work/policy/wellbeing/new-filters.html](http://www.rsph.org.uk/our-work/policy/wellbeing/new-filters.html) Report by the All Party Parliamentary Group (APPG) on Social Media on the Group's Inquiry, "#NewFilters to manage the impact of social media on young people's mental health and wellbeing". This is the first national Inquiry specifically examining the impact of social media on the mental health and wellbeing of young people, which ran from April 2018 to January 2019.

[www.thinkuknow.co.uk/professionals/](http://www.thinkuknow.co.uk/professionals/) Supporting you to deliver education and raise awareness of digital child exploitation and abuse.

[www.thinkuknow.co.uk/professionals/guidance/digital-romance/](http://www.thinkuknow.co.uk/professionals/guidance/digital-romance/) This research project looks at how young people use technology in developing romantic relationships and surviving break ups. The project was led by Brook, the UK's leading sexual health and wellbeing charity for under 25s, and the CEOP Command of the NCA.

[www.tes.com/teaching-resource/digital-citizenship-young-peoples-rights-on-social-media-teaching-pack-for-11-14-year-olds-11734349](http://www.tes.com/teaching-resource/digital-citizenship-young-peoples-rights-on-social-media-teaching-pack-for-11-14-year-olds-11734349) Digital citizenship: Young peoples' rights on social media – a teaching pack designed to help pupils aged 11 to 14 develop the resilience, power and information they need to thrive online. This teaching pack comprises a short, six-lesson unit of work written by teacher and citizenship specialist Emily Cotterill.

[www.nen.gov.uk/digital-safety](http://www.nen.gov.uk/digital-safety) Leading educational support for helping you stay safe digitally.

<https://educateagainsthate.com/> This website gives [teachers](#), [parents](#) and [school leaders](#) practical advice and information on protecting children from extremism and radicalisation.

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/440450/How\\_social\\_media\\_is\\_used\\_to\\_encourage\\_travel\\_to\\_Syria\\_and\\_Iraq.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/440450/How_social_media_is_used_to_encourage_travel_to_Syria_and_Iraq.pdf) This briefing note is aimed at head teachers, teachers and safeguarding leads and provides advice about digital terrorist and extremist material.

[www.mercurynews.com/2017/09/21/how-to-combat-lgbtq-cyberbullying](http://www.mercurynews.com/2017/09/21/how-to-combat-lgbtq-cyberbullying) Article on combating LGBTQ+ bullying.

<https://www.barnardos.org.uk/campaign-with-us/childrens-social-media-and-mental-health> Report on children's social media and mental health.

<https://www.gov.uk/government/publications/sexting-in-schools-and-colleges> 'Sexting' in schools: advice and support around self-generated images. This advice is for designated safeguarding leads (DSLs), their deputies, head teachers and senior leadership teams in schools and educational establishments.

[www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/650933/Literature\\_Review\\_Final\\_October\\_2017.pdf](http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/650933/Literature_Review_Final_October_2017.pdf) Children's digital activities, risks and safety. A literature review by the UKCCIS (UK Council for Child Internet Safety) Evidence Group. October 2017.

<https://www.gov.uk/government/publications/digital-resilience-framework> A framework and tool for organisations, policymakers, schools and companies to use to embed digital resilience thinking into products, education and services.

The NSPCC Knowledge and Information Services provide newsletters and updates on safeguarding research, including digital safety. Information can be found at [www.nspcc.org.uk/library](http://www.nspcc.org.uk/library) CASPAR (Current Awareness Service for Policy, Practice and Research) is the NSPCC's weekly email update delivering the latest news in child protection policy, practice and research, every Monday. Sign up to CASPAR at [www.nspcc.org.uk/caspar](http://www.nspcc.org.uk/caspar) or you can follow them on Twitter @NSPCCpro. The NSPCC also provide specialist child protection courses (introductory, advanced and specialist) either online or face-to-face [www.nspcc.org.uk/training](http://www.nspcc.org.uk/training)