# E-SAFETY POLICY

| | | | |
|---|---|---|---|
| **Author:** | Heather Murphy<br>(Assistant Headteacher- Safeguarding and Attendance<br>Designated Safeguarding Lead<br>Senior Mental Health Lead) | | |
| **Reviewed:** | Summer 2026<br>(Biennial) | **Next review due:** | Summer 2028 |
| **Approved by:** | Andrea Bell | **Date approved:** | July 2026 |


Aims.

Legislation and guidance.

Roles and responsibilities.

Educating pupils about online safety.

Educating parents/carers about online safety.

Cyber-bullying.

Acceptable use of the internet in school.

Pupils using mobile devices in school.

Staff using work devices outside school.

Technical – infrastructure/equipment, filtering and monitoring.

How school will respond to issues of misuse.

Training.

Monitoring arrangements.

Links to other policies.

Appendix 1: acceptable use agreement (pupils and parents/carers)

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Appendix 3: online safety training needs – self audit for staff

## 1. Aims

At NRA we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

**The 4 Key Categories of Risk**

Our approach to online safety is based on addressing the following categories of risk:

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

## 2. Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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. The policy also takes into account the National Curriculum computing programmes of study.

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

## 3. Roles and responsibilities

### 3.1 The Governing Body

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

The governing body 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 governing body 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 governing body 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 governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body 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 ICT manager and service providers what needs to be done to support the school in meeting the 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 governor who oversees online safety is the Lead Governor for Safeguarding: Sue Wright.

All governors 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 3)

Ensure that online safety is a running and interrelated theme while devising and implementing their whole school 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

### 3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### 3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions. 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 and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

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 on school devices and school networks, which are reviewed and updated at least annually 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
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers 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 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 or processes failing by alerting the ICT manager and team and DSL via email. If the report has an impact on the safeguarding of students, this will be logged on CPOMs.
- Following the correct procedures by requesting access via the ICT manager and team if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- 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 could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

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
- Parent resource sheet – Childnet

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 (appendix 3).

## 4. Educating pupils about online safety

The aim of our approach to online safety is empowerment to protect and educate pupils and staff in their use of technology and establish mechanisms to identify, intervene in, and escalate any concerns where appropriate. We will ensure appropriate filtering and monitoring on school/ devices and networks. We aim to protect children from illegal, inappropriate or harmful content, and harmful online interaction with other users. We aim for our pupils to exhibit positive personal online behaviour and recognise inappropriate online conduct. We aim to protect children from commercial risks.

We embed the teaching of online safety through the ICT curriculum and via Personal Development (PD) lessons involving online safety.

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 to child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; 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 we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group (https://apwg.org/).

We will ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety while planning the curriculum, any teacher training, the role and responsibilities of the DSL (and deputies) and any parental engagement. Our approach to online safety is reflected within this policy and includes the role of the Lead DSL in ensuring that there is appropriate filtering and monitoring of school devices and school networks.

Pupils will be taught about online safety as part of the curriculum:

**All schools have to teach:**

- Relationships and sex education and health education in secondary schools

**In KS3, 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 KS4 will be taught:**

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

**By the end of secondary school, pupils will know:**

- 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 that 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 that 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. 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

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

Online safety will also be covered during parents' evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

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

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

**6.2 Preventing and addressing cyber-bullying**

Our NRA values of ambition, respect, courage reflect the importance of ensuring that all members of our school community are protected from cyber-bullying.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others.

We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.

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 (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

**6.3 Examining electronic devices (including mobile phones, laptops, iPads and any other electronic device)**

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher and/or Lead DSL.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or seminude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Child Protection and Safeguarding Policy
- Our Behaviour Policy

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

### 6.4 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.

NRA 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

NRA will treat any use of AI to bully pupils in line with our Behaviour Policy and Child on Child 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 the Trust.

## 7. Acceptable use of the internet in school

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 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Pupils using mobile devices in school

**Mobile Phones**

The school follows the 2024 Government Guidance for Mobile Phone use in school. We follow the guidance that mobile phones should be **never used, seen or heard**.

Students are not permitted to have a mobile phone visible on the premises. Any student visibly in possession of a mobile phone will have it confiscated immediately and their parents/carers may be called to collect it from school for repeat offences. Phones must never be taken into internal or public examinations.

When it is suspected that a mobile phone has been used for inappropriate purposes such as cyber bullying etc. the school has the right to read, copy or delete messages. The phone will be

confiscated and returned once parents are informed of the issues. (Links to the DFE document "Screening, Searching and Confiscation 2022")

**e-Watches/iPods/Music Players**

Students may not use these at school; other than e-Watches for time telling purposes.

**Online Media Presence**

Students are not permitted to make reference to the school, staff or students in social media, for example TikTok Youtube and Instagram.. This includes comments, photographs and naming members of New Road Academy. Any student found to have posted material online which refers in any way to NRA, will be at risk of permanent exclusion.

## 9. Staff and Visitor Mobile Phone and Electronics Use

We recognise that staff and visitors are likely to bring a mobile phone onto the school site. The expectation for staff is their phone is stored away and not left out on display. Staff are not allowed to take photographs of children on their personal electronic devices. Acceptable mobile phone use information is shared with visitors who are asked to keep their phones stored away.

All teaching staff and teaching assistants have a school laptop. These have been built by the Telford and Wrekin ICT department so are set with appropriate filters. Staff have to input their individual login details in order to get into the computer. A select group of staff (SLT and pastoral staff) have a school provided mobile phone. These have been built by the Telford and Wrekin ICT department.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

## 10. Technical – infrastructure / equipment, filtering and monitoring

### 10.1 Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

The Online Safety Policy is consistent with and inter-related to other relevant school polices including but not limited to:

- NRA Child Protection and Safeguarding Policy
- Behaviour for Learning Policy
- Anti-Bullying & Child on Child Policy
- Acceptable Use Policy

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education curriculum via IT/Computing and PD.

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

The school allows:

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

** Authorised device – purchased by the student/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.*

### 10.2 Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of

the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press

• In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital video /images.

• Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital video/images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Student's work can only be published with the permission of the student and parents or carers.

**10.3 Data Protection**

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document. Schools should ensure that

they take account of policies and guidance provided by local authorities / MAT / or other relevant bodies.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

• It has a Data Protection Policy.

• It has paid the appropriate fee to the Information Commissioner's Office (ICO).

• It has appointed a Data Protection Officer (DPO). The Schools appointed DPO is: Mr David Hubbard, Business Manager – 01952 386400

• The Lead Officer for the Learning Community Trust for GDPR is Mr Paul Jones - 01952 387010

• It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

• Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.

• The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.

• Where special category data is processed, a lawful basis and a separate condition for processing have been identified.

• Data Protection Impact Assessments (DPIA) are carried out.

• It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.

• Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

• There are clear and understood data retention policies and routines for the deletion and disposal of data.

• There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.

• Consideration has been given to the protection of personal data when accessed using any remote access solutions.

• All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.

• All staff receive data handling awareness/data protection training and are made aware of their responsibilities.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

• The data must be encrypted and password protected.

• The device must be password protected.

• The device must offer approved virus and malware checking software.

• The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

**10.4 Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| | Staff & other adults | Students |
|---|---|---|

| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission |
|---|---|---|---|---|---|---|---|---|
| Mobile phones may be brought to the school | * | | | | * | | | |
| Use of mobile phones in lessons | | | * | | * | | | |
| Use of mobile phones in social time | * | | | | * | | | |
| Taking photos on mobile phones / cameras | | | | * | * | | | |
| Use of other mobile devices eg: tablets, gaming devices | * | | | | | | | * |
| Use of personal email addresses in school, or on school network | | | | * | * | | | |
| Use of school email for personal emails | | | | * | * | | | |
| Use of messaging apps | | | * | | | | | * |
| Use of social media | | | * | | * | | | |
| Use of blogs | | | * | | | | | * |

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

• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

• Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

• Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official monitored school systems. Personal email addresses, text messaging or social media must not be used for these communications.

• Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

**10.5 Social Media - Protecting Professional Identity**

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for and staff. Schools, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to staff and the school through:

• Ensuring that personal information is not published

• Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.

• Clear reporting guidance, including responsibilities, procedures and sanctions

Risk assessment, including legal risk School staff should ensure that:

• No reference should be made in social media to students, parents/carers or school staff

• They do not engage in online discussion on personal matters relating to members of the school community

• Personal opinions should not be attributed to the school or local authority/MAT

• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established, there should be:

• A process for approval by senior leaders

• Clear processes for the administration and monitoring of these accounts – involving at least two members of staff

• A code of behaviour for users of the accounts, including

• Systems for reporting and dealing with abuse and misuse

• Understanding of how incidents are dealt with under school disciplinary procedures

Personal Use:

• Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

• Personal communications which do not refer to or impact upon the school are outside the scope of this policy

• Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

• The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media

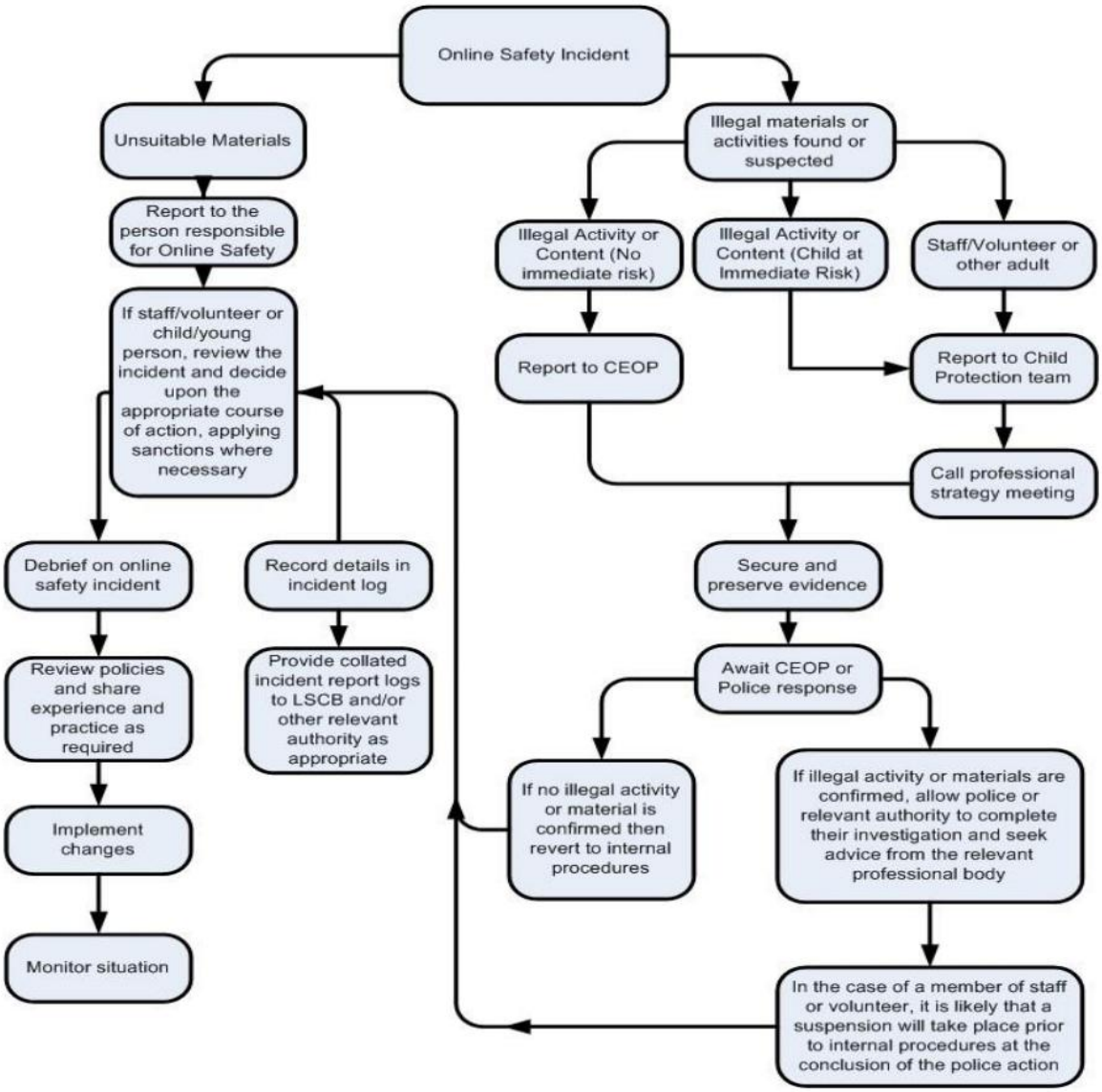
• As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

• The school should effectively respond to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

## 11.How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. 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 ICT 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 code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

## 12. Training

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

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - o Abusive, threatening, harassing and misogynistic messages
    - o Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - o 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:

• 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 up the risks

• 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 deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

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.

## 13. Monitoring arrangements

The school uses SENSO to monitor online safety on devices in school. The DSL or relevant staff member dealing with an incident logs behaviour and safeguarding issues related to online safety via CPOMs.

The Online Safety Policy will be reviewed every year by the Lead DSL in conjunction with the Subject Leader for IT and the ICT Manager. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: NRA Acceptable Use Agreement (pupils and parents/carers)

**See LCT ICT Acceptable Use Policy, Learner Acceptable Use Policy Agreement KS3/KS4**

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

**See LCT ICT Acceptable Use Policy, ICT Acceptable Use Policy Agreement (Staff and all other users)**

Appendix 3: online safety training needs – self-audit for staff

**Staff undergo Educare GDPR training on an annual basis, and SmartLog Basic GDPR and GDPR in Education every other year.**