Online Safety Policy

September 2022

Contents: **Page no:**

Linton School

Online Safety Policy

Adopted by: Rebekah Dennett **Review date:** September 2022

Designated Safeguard Lead: Rebekah Dennett

Deputy Designated Safeguard Lead: Sean Di Sora & Paul Barton

Head Teacher: Rebekah Dennett

Regional Lead: Declan Tuer

The Designated Safeguarding Lead is: Rebekah Dennett
Contact email: Rebekah.dennett@rocnorthwest.co.uk
Tel: 01772 957062 / 07776 528079

Regional Lead: Declan Tuer
Contact email: Declan.tuer@caretech-uk.com
Tel: 07827 302334

The Deputy Designated Safeguarding Lead is: Sean Di Sora
Contact email: sean.disora@lintonschool.co.uk
Tel: 01772 957062
The Deputy Designated Safeguarding Lead is: Paul Barton
Contact email: paul.barton@lintonschool.co.uk
Tel: 01772 957062
The LA Designated Officer for Lancashire County Council is: Tim Booth
Contact email: tim.booth@lancashire.gov.uk
Tel: 01772 536694
The LA Designated Officer for Blackpool Council is: Amanda Quirke
Contact email: Amanda.quirke@blackpool.gov.uk
Tel: 01253 477541

Lancashire County Council – School Safeguarding Helpline: 01772 531196
Lancashire County Council – Emergency Duty Team: 0300 123 6722 (out of office hours)

Blackpool Council – Multi-Agency Safeguarding Hub (MASH): 01253 477299
If the child is at immediate risk, please call the police on 999.

Our School

Linton School is an independent special school for young people with social, emotional and mental health difficulties for both boys and girls aged 8-18 years old. The school is registered for up to 12 learners and consists of 4 small classes to provide a nurturing environment to develop and progress throughout their learning journey. We are a trauma informed school that is able to support children and teenagers who suffer with trauma or mental health problems and whose troubled behaviour acts as a barrier to learning. Located in rural Preston we therefore benefit from some amazing outdoor space where we develop our outdoor, equestrian and horticulture skills. All the staff at Linton School are committed to creating a setting which not only focuses on academic success, but also provides our learners opportunities to develop their social, communication and independent skills.

Culture and Ethos

We are committed to providing a nurturing, safe and ambitious learning environment that supports every young person to achieve lifelong skills through a diverse learner centred curriculum. Respectful and supportive relationships are at the heart of all we do; we value every member of the school community equally. Through bespoke curriculums tailored towards each individual pupil's needs, experiences, interests and strengths we foster a love for learning and support our young people to achieve their full potential. As an educational setting our main aim is to prepare our pupils to make a positive contribution towards society by giving our students the skills they need to be successful, resilient and inspirational young adults. Linton schools purpose is to improve the quality of life for our young people both now, and in the future, 'building our futures together'.

The Vision

Linton School provides a safe, nurturing learning environment to provide skills for lifelong opportunities, which gives the young people an ambitious outlook towards their future.

The vision drives everything we do and will be achieved through:

- Outdoor enrichment activities to promote life skills through play, nurture and teamwork.
- Promoting independence, patience and listening skills through Equestrian lessons.
- Multi-disciplinary links from both internal and external companies to provide a bespoke, broad and balanced curriculum that develops the education of our pupils.
- Empowering each learner to achieve their personal goals and develop a lifelong love of learning.
- A positive and ambitious school environment that promotes learning for all.
- Offering a broad range of learning experiences within the curriculum that values academic attainment as well as developing social skills, experiences and resilience.

More information about the school can be found in the school Prospectus.

1. Aims

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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) 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.

3. Introduction

The purpose of having Internet access in School:

The purpose of the Internet access in school is to increase the opportunities for learners to access a wider range of resources in support of the curriculum. It supports the professional work of staff and enhances the school's management information and business administration practice. Access to the school network and the Internet is necessary for staff and learners. It is an entitlement for all learners as it helps them to develop a responsible and mature approach to accessing information. Access to internet, ICT and digital media, in order to provide opportunities for technology enhanced

learning, forms part of all school inspections under the Common Inspection Frameworks in England and Wales.

What are the benefits to the School?

Following a number of studies it has been determined that there are defined benefits to be gained through the appropriate use of the ICT systems, including the Internet, in education. These benefits include:

- Access to worldwide educational resources including museums and art galleries;
- Information and cultural exchanges between learners world-wide;
- News, current events and archive material;
- Cultural, social and leisure use in libraries, clubs and at home;
- Discussion with experts in many fields for learners and staff;
- Staff professional development with access to educational materials and curricula;
- Communication with the advisory and support services, local authorities and agencies.

Therefore at Linton School, pupils are educated and supported to access the internet and digital learning resources safely and appropriately, and in order to enrich the learning opportunities available to them.

4. Roles and Responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online 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 ICT systems and the internet
- 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

The Head Teacher

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

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our Safeguarding and Child Protection policy.

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

- Supporting the Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher, 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 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head Teacher and/or governing board

This list is not intended to be exhaustive.

The ICT Manager

The ICT Manager for Linton School is Sean Di Sora.

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
- 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 (see appendix 5) 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.

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, and ensuring that pupils follow the school's terms on acceptable use
- 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.

Parents

Parents are expected to:

- Notify a member of staff or the Head Teacher 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 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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

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.

5. Educating pupils about online safety

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

Linton School will also teach:

- Relationships education and health education to primary ages students and;
- Relationships and sex education and health education to secondary ages pupils.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of Key Stage 2**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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:

- 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 Key Stage 4**, 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 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.

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

Educating parents about online safety

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

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

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

6. Allegations of abuse made against other pupils

We recognise that children are capable of abusing their peers. Abuse will never be tolerated or passed off as "banter", "just having a laugh" or "part of growing up", as this can lead to a culture of unacceptable behaviours and an unsafe environment for pupils.

We also recognise the gendered nature of peer-on-peer abuse. However, all peer-on-peer abuse is unacceptable and will be taken seriously.

Most cases of pupils hurting other pupils will be dealt with under our school's Behaviour Policy, but this Safeguarding and Child Protection policy will apply to any allegations that raise safeguarding concerns. This might include where the alleged behaviour:

- Is serious, and potentially a criminal offence
- Could put pupils in the school at risk
- Is violent
- Involves pupils being forced to use drugs or alcohol
- Involves sexual exploitation, sexual abuse or sexual harassment, such as indecent exposure, sexual assault, upskirting or sexually inappropriate pictures or videos (including the sharing of nudes and semi-nudes)

All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). This is most likely to include, but may not be limited to:

- bullying (including cyberbullying);
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm;
- sexual violence, such as rape, assault by penetration and sexual assault;
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse;
- upskirting, which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm;
- sexting (also known as youth produced sexual imagery); and
- initiation/hazing type violence and rituals.

Sexual violence and sexual harassment between children in schools and colleges

Sexual violence and sexual harassment can occur between two children of any age and sex. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and offline (both physical and verbal) and are never acceptable. It is important that all victims are taken seriously and offered appropriate support. Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with SEND and LGBT children are at greater risk.

Staff should be aware of the importance of:

- making clear that sexual violence and sexual harassment is not acceptable, will never be tolerated and is not an inevitable part of growing up;
- not tolerating or dismissing sexual violence or sexual harassment as "banter", "part of growing up", "just having a laugh" or "boys being boys"; and
- challenging behaviours (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them.

Sexual violence

It is important that school and college staff are aware of sexual violence and the fact children can, and sometimes do, abuse their peers in this way. When referring to sexual violence we are referring to sexual violence offences under the Sexual Offences Act 2003109 as described below:

- **Rape:** A person (A) commits an offence of rape if: he intentionally penetrates the vagina, anus or mouth of another person (B) with his penis, B does not consent to the penetration and A does not reasonably believe that B consents.
- **Assault by Penetration:** A person (A) commits an offence if: s/he intentionally penetrates the vagina or anus of another person (B) with a part of her/his body or anything else, the penetration is sexual, B does not consent to the penetration and A does not reasonably believe that B consents.
- **Sexual Assault:** A person (A) commits an offence of sexual assault if: s/he intentionally touches another person (B), the touching is sexual, B does not consent to the touching and A does not reasonably believe that B consents.

What is consent?

Consent is about having the freedom and capacity to choose. Consent to sexual activity may be given to one sort of sexual activity but not another, e.g.to vaginal but not anal sex or penetration with conditions, such as wearing a condom. Consent can be withdrawn at any time during sexual activity and each time activity occurs. Someone consents to vaginal, anal or oral penetration only if s/he agrees by choice to that penetration and has the freedom and capacity to make that choice.

Sexual harassment

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline. When we reference sexual harassment, we do so in the context of child on child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names;
- sexual "jokes" or taunting;
- physical behaviour, such as: deliberately brushing against someone, interfering with someone's clothes (schools and colleges should be considering when any of this crosses a line into sexual violence - it is important to talk to and consider the experience of the victim) and displaying pictures, photos or drawings of a sexual nature; and
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
    - non-consensual sharing of sexual images and videos;
    - sexualised online bullying;
    - unwanted sexual comments and messages, including, on social media;
    - sexual exploitation; coercion and threats; and
    - upskirting.

Upskirting

'Upskirting' typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is now a criminal offence.

The response to a report of sexual violence or sexual harassment

The initial response to a report from a child is important. It is essential that all victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report.

If staff have a concern about a child or a child makes a report to them, they should follow Linton School's Safeguarding and Child Protection policy. As is always the case, if staff are in any doubt as to what to do they should speak to the Designated Safeguarding Lead (or a deputy).

Sharing of nudes and semi-nudes (sexting)

Your responsibilities when responding to an incident

If you are made aware of an incident involving the consensual or non-consensual sharing of nude or semi-nude images/videos (also known as 'sexting' or 'youth produced sexual imagery'), you must report it to the DSL immediately.

You must **not**:

- View, copy, print, share, store or save the imagery yourself, or ask a pupil to share or download it (if you have already viewed the imagery by accident, you must report this to the DSL)
- Delete the imagery or ask the pupil to delete it
- Ask the pupil(s) who are involved in the incident to disclose information regarding the imagery (this is the DSL's responsibility)
- Share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- Say or do anything to blame or shame any young people involved

You should explain that you need to report the incident, and reassure the pupil(s) that they will receive support and help from the DSL.

Please see Linton School's Safeguarding and Child Protection, Behaviour and Online Safety policy for more details.

Procedures for dealing with allegations of peer-on-peer abuse

If a pupil makes an allegation of abuse against another pupil:

- You must record the allegation and tell the DSL, but do not investigate it
- The DSL will contact the local authority children's social care team and follow its advice, as well as the police if the allegation involves a potential criminal offence
- The DSL will put a risk assessment and support plan into place for all children involved (including the victim(s), the child(ren) against whom the allegation has been made and any others affected) with a named person they can talk to if needed
- The DSL will contact the Children and Adolescent Mental Health services (CAMHS), if appropriate

Creating a supportive environment in school and minimising the risk of peer-on-peer abuse

We recognise the importance of taking proactive action to minimise the risk of peer-on-peer abuse, and of creating a supportive environment where victims feel confident in reporting incidents.

To achieve this, we will:

- Challenge any form of derogatory or sexualised language or inappropriate behaviour between peers, including requesting or sending sexual images
- Be vigilant to issues that particularly affect different genders – for example, sexualised or aggressive touching or grabbing towards female pupils, and initiation or hazing type violence with respect to boys

- Ensure our curriculum helps to educate pupils about appropriate behaviour and consent
- Ensure pupils are able to easily and confidently report abuse using our reporting systems
- Ensure staff reassure victims that they are being taken seriously
- Ensure staff are trained to understand:
    - How to recognise the indicators and signs of peer-on-peer abuse, and know how to identify it and respond to reports
    - That even if there are no reports of peer-on-peer abuse in school, it does not mean it is not happening – staff should maintain an attitude of "it could happen here"
    - That if they have any concerns about a child's welfare, they should act on them immediately rather than wait to be told, and that victims may not always make a direct report. For example:
        - Children can show signs or act in ways they hope adults will notice and react to
        - A friend may make a report
        - A member of staff may overhear a conversation
        - A child's behaviour might indicate that something is wrong
    - That certain children may face additional barriers to telling someone because of their vulnerability, disability, gender, ethnicity and/or sexual orientation
    - That a pupil harming a peer could be a sign that the child is being abused themselves, and that this would fall under the scope of this policy
    - The important role they have to play in preventing peer-on-peer abuse and responding where they believe a child may be at risk from it
    - That they should speak to the DSL if they have any concerns

Initial review meeting

Following a report of an incident, the DSL will hold an initial review meeting with appropriate school staff – this may include the staff member who reported the incident and the safeguarding or leadership team that deals with safeguarding concerns. This meeting will consider the initial evidence and aim to determine:

- Whether there is an immediate risk to pupil(s)
- If a referral needs to be made to the police and/or children's social care
- If it is necessary to view the image(s) in order to safeguard the young person (in most cases, images or videos should not be viewed)
- What further information is required to decide on the best response
- Whether the image(s) has been shared widely and via what services and/or platforms (this may be unknown)
- Whether immediate action should be taken to delete or remove images or videos from devices or online services
- Any relevant facts about the pupils involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved (in most cases parents/carers should be involved)

The DSL will make an immediate referral to police and/or children's social care if:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
- What the DSL knows about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the images or videos is under 13
- The DSL has reason to believe a pupil is at immediate risk of harm owing to the sharing of nudes and semi-nudes (for example, the young person is presenting as suicidal or self-harming)

If none of the above apply then the DSL, in consultation with the Head Teacher and other members of staff as appropriate, may decide to respond to the incident without involving the police or children's social care. The decision will be made and recorded in line with the procedures set out in this policy.

Further review by the DSL

If at the initial review stage a decision has been made not to refer to police and/or children's social care, the DSL will conduct a further review to establish the facts and assess the risks.

They will hold interviews with the pupils involved (if appropriate).

If at any point in the process there is a concern that a pupil has been harmed or is at risk of harm, a referral will be made to children's social care and/or the police immediately.

Informing parents

The DSL will inform parents at an early stage and keep them involved in the process, unless there is a good reason to believe that involving them would put the pupil at risk of harm.

Referring to the police

If it is necessary to refer an incident to the police, this will be done through by dialing 101 and in line with the new NPCC document 'When to call the police'.

Recording incidents

All incidents of sharing of nudes and semi-nudes, and the decisions made in responding to them, will be recorded.

Curriculum coverage

Pupils are taught about the issues surrounding the sharing of nudes and semi-nudes as part of our Relationships and Sex Education and computing programmes. Teaching covers the following in relation to the sharing of nudes and semi-nudes:

- What it is
- How it is most likely to be encountered
- The consequences of requesting, forwarding or providing such images, including when it is and is not abusive and when it may be deemed as online sexual harassment
- Issues of legality
- The risk of damage to people's feelings and reputation

Pupils also learn the strategies and skills needed to manage:

- Specific requests or pressure to provide (or forward) such images
- The receipt of such images

7. Bullying and Cyber-Bullying

Bullying definition

Bullying is hurtful, unkind or threatening behaviour which is deliberate and repeated.

Bullying can be carried out by an individual or a group of people towards another individual or group, where the bully or bullies hold more power than those being bullied. If bullying is allowed it harms the perpetrator, the target and the whole school community. The vision and values of the school should lead to a diminishing of any such behaviour.

The Anti-Bullying Alliance defines bullying as: "The repetitive, intentional hurting of one person or group by another person or group, where the relationship involves an imbalance of power" (2015). It can happen face-to-face or through cyberspace (on-line, via social media or texting).

We make reference to the acronym below to help children understand that bullying is hurtful behaviour that happens:

- **S**everal
- **T**imes
- **O**n
- **P**urpose

The nature of bullying can be:

- Physical (e.g. hitting, kicking, pushing or inappropriate/unwanted physical contact)
- Verbal (e.g. name calling, ridicule, comments)
- Cyber (e.g. messaging, social media, email)
- Emotional/indirect/segregation (e.g. excluding someone, spreading rumours)
- Visual/written (e.g. graffiti, gesture, wearing racist insignia)
- Damage to personal property
- Threat with a weapon
- Theft of extortion
- Persistent bullying

Bullying could be based on many things, including:

- Race
- Religion or belief
- Special Educational Needs or disability
- Culture or class
- Appearance or health conditions
- Sexual orientation or Gender identity (homophobic, biphobic, transphobic)
- Gender
- Related to home or other personal circumstances

Responding to bullying

1. Staff will record the bullying incident centrally on Behaviour Watch.
2. The Head Teacher, Rebekah Dennett will monitor incident reporting on Behaviour Watch.
3. If an incident does occur the designated school staff will produce a report summarising the information which the Head Teacher will report to the governing body.

4. Support will be offered to the victim of the bullying from staff within the school setting.
5. Staff will proactively respond to the bully who may require support from the Occupational Therapists, Speech and Language Therapists or the Counsellor.
6. Staff will assess whether parents and carers need to be involved.
7. Staff will assess whether any other authorities (such as police or local authority) need to be involved, particularly when actions take place outside of school.

Bullying outside of school

Within Linton School Educational Provision we do not tolerate injustice and bullying whether it takes place inside or outside of school. The nature of cyber bullying in particular means that it can impact on pupils beyond the school day. Staff, parents, carers, and pupils must be vigilant to bullying outside of school and report and respond according to their responsibilities outlined in this policy.

The school is active in addressing responsible and respectful use of social media. The school is active in supporting parents and carers to take responsibility for their child's respectful use of social media especially in such a fast changing environment. Staff will assess whether any other authorities (such as police or local authority) need to be involved.

Cyber-Bulling 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 one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

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

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.

School's strategies to prevent and tackle bullying

We use a range of measures to prevent and tackle bullying including:

- Our school vision is at the heart of everything we do and ensures that all members of the school community are revered and respected as members of a community.
- We use a pupil-friendly information to ensure that all pupils understand what bullying is and know how to report bullying.
- The whole school curriculum is used to highlight and explore the anti-bullying commitment of the school. There are more extensive opportunities to explore anti-bullying themes within the PSHE programme of study which includes opportunities for pupils to understand about different types of bullying and what they can do to respond and prevent bullying.
- Bespoke curriculums explore the importance of inclusivity, dignity and respect as well as other themes that play a part in challenging bullying.
- Through a variety of planned activities and time across the curriculum pupils are given the opportunity to gain self-confidence and develop strategies to speak up for themselves and express their own thoughts and opinions.
- Form time provides regular opportunities to discuss issues that may arise in class and for teachers to target specific interventions.
- Stereotypes are challenged by staff and pupils across the school.
- Restorative justice systems provide support to victims of bullying and those who show bullying behaviour.
- Pupils are continually involved in developing school-wide anti-bullying initiatives through consultation with the school council.
- Working with parents and carers, and in partnership with community organisations to tackle bullying where appropriate.

Please see Linton School's Anti-Bullying, Behaviour policy for more details.

8. 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.

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
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

- The school's COVID-19 risk assessment

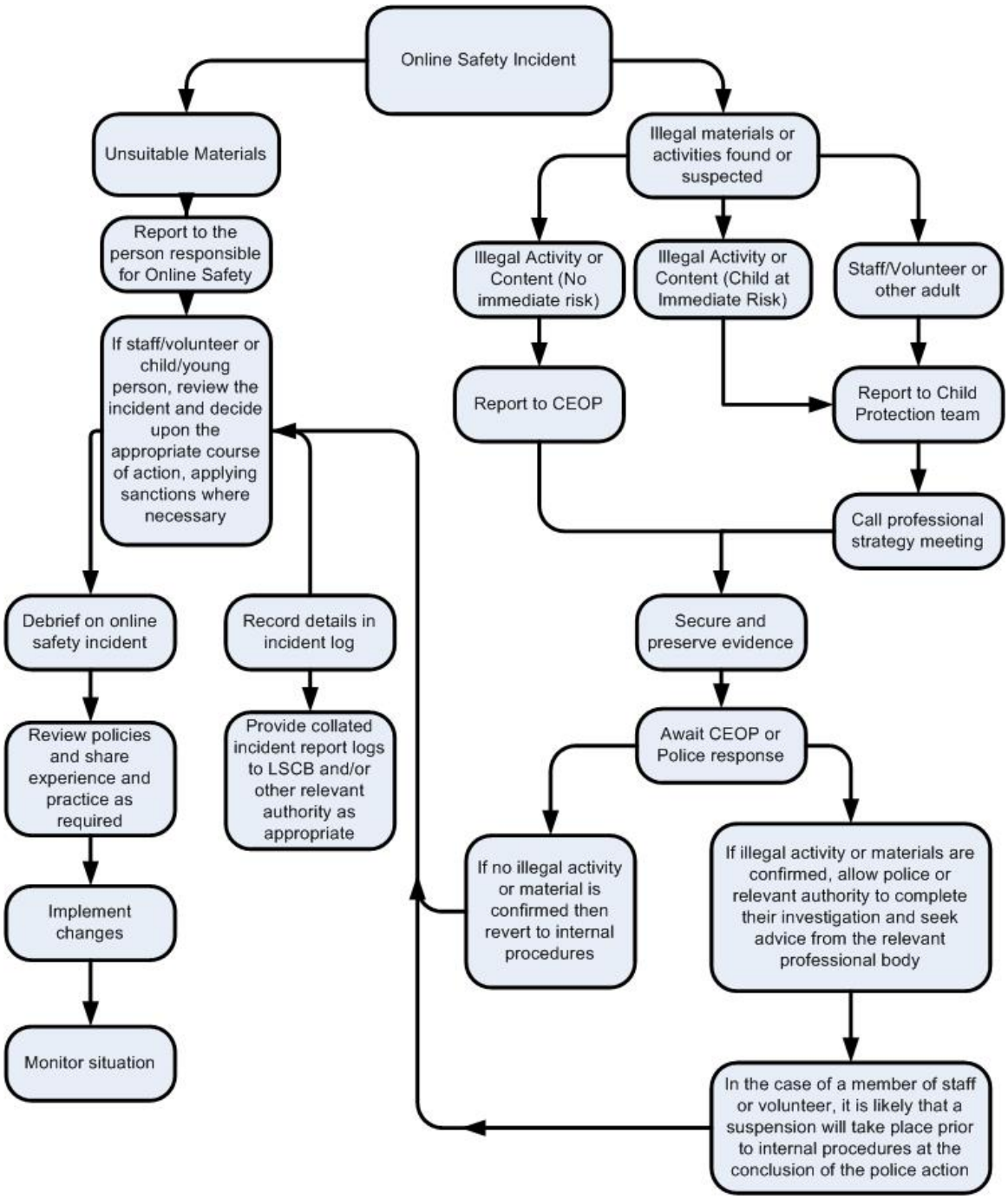
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

9. Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents:
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this investigation procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the investigation form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school, and possibly the police, and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed investigation form should be retained by the school for evidence and reference purposes.

10. Filtering and Monitoring

The schools will be responsible for ensuring that the schools' infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

Additionally, schools will need to liaise and communicate effectively with CareTech IT Support Services in order to ensure that all corporate infrastructure/network relevant to the school is as safe and secure as reasonably possible, and in order to ensure that schools can maintain their duty of safeguarding to all pupils.

CareTech IT Support Services must ensure that:

- The Schools' technical systems and infrastructure are managed in ways that ensure that the schools technical requirements meet the required standard to ensure effective safeguarding of all pupils;
- There are regular reviews and audits of the safety and security of schools technical systems;
- Servers, wireless systems and cabling are securely located and physical access restricted;
- All users have clearly defined access rights to a school's technical systems and devices;
- All users (at KS2 and above) are provided with a username and secure password by IT Support, who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at a time decided by IT Support;
- The "administrator" passwords for the schools' ICT systems, used by the Network Manager (or other person) must also be available to the Head teacher, and kept in a secure place;
- That software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes; (Go-Guardian is the schools monitoring and filter application).
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. Note: additional duties exist for schools under the Counter Terrorism and Securities Act 2015, which requires schools to ensure that children are safe from terrorist and extremist material on the internet;
- The school has enhanced / differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc);
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;

The schools must ensure that:

- School staff regularly monitor and record the activity of users on the schools' systems and users are made aware of this in the Acceptable Use Agreement;
- An appropriate system is in place for users to report any actual or potential incident or security breach to the relevant person, as agreed;
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems;
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school;
- An agreed policy is in place that allows staff to, or forbids staff from, downloading executable files and installing programmes on school devices;
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/ DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off

the school site unless safely encrypted or otherwise secured. (see Schools' Data Protection Policy).

11. Mobile Technologies (including BYOD)

Mobile technology devices may be school owned or provided 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 network, or cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile devices in a school context is educational. This policy is consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Agreement, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

The school Acceptable Use Agreements for staff, pupils and carers will give consideration to the use of mobile technologies.

School Owned Devices:
The school has mobile technology devices available for use as learning tools in the school day. These include laptops and tablets. School owned devices are managed in the following way:

- Devices are allocated to pupils and staff for education and training purposes;
- Devices are allocated by the head teacher, ICT teacher or classroom teacher for use in the school, at a specific time, and for a designated purpose;
- Unsupervised personal use is NOT permitted;
- Network access is controlled by the parameters created by the user level assigned to a username; also by Go-Guardian protection.
- All internet access is security protected with a password, and supervised by staff;
- The Head teacher and ICT teacher are responsible for the management of devices, settings, installation of software and apps, and monitoring use; this is controlled by Go-Guardian.
- Technical support is provided by CareTech IT Support Services
- Filtering of devices is administered by CareTech IT Support Services, using Net Nanny and also Go-Guardian.
- Pupil work should be stored within the local network on the pupil's user account, and not stored on individual devices;
- Pupils and staff may be held liable for intentional damage to school devices.

Personal devices:

- Pupils are allowed personal mobile devices in school to be used at break times only, unless agreed by the Head teacher to be used at other times;
- Teachers and support staff are not allowed to use personal mobile devices during school time, other than at prescribed break times, or in the event of an emergency;
- The Head Teacher and Deputy Head teacher are allowed access to their personal or work mobile devices during school time, in order to fulfil their work commitments;
- Any personal mobile devices brought into school by pupils must be handed in and kept in the Head teachers office until the end of the school day, unless stated otherwise by the Head teacher;

- The Head Teacher will decide whether staff will be allowed to use personal devices for school business;
- All internet access is security protected with a Wi-Fi password, and supervised by staff. All pupils or staff accessing the Wi-Fi will be subject to filtering and monitoring by Net Nanny and Go-Guardian;
- Personal devices must not be used to store any personal data relating to the workplace;
- Personal devices must not be used to record video or digital images of pupils or staff in the workplace;
- Liability for loss/damage or malfunction of personal devices rests with the owner of the personal device;
- Staff personal devices must not be shared with pupils or used to allow them access to the internet;
- Visitors will be informed of their responsibilities in regards to bringing personal devices onto school site.

Communication devices:

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:

Use of Communication Devices	**Staff & Other Adults**				**Pupils**			
	Not Allowed	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**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 e.g. tablets, gaming devices			✓				✓	

Use of personal email addresses in school , or on school network			✓		✓			
Use of school email for personal emails	✓				✓			
Use of social media			✓			✓	✓	
Use of blogs			✓			✓	✓	
Use of messaging apps			✓			✓	✓	

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

- The official company email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff 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 pupils 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/academy systems. Personal email addresses, text messaging or social media **must not be used** for these communications.
- Pupils 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 **must not** be posted on the school website and only official email addresses should be used to identify members of staff.

12. Use of Video and Digital Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, carers and pupils 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 to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils 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 consent from the pupil or the corporate parent will be obtained before photographs of pupils 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 pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff **must not** be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

13. Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed, following the European Union General Data Protection Regulation (GDPR). As a result, schools are subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the schools' Data Protection Policy.

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

The school must ensure that:

- It has a Data Protection Policy.
- CareTech are registered as a data controller with the ICO. All schools operate within CareTech registration.
- There is a corporate Data Protection Officer, but the Head Teacher in each school has the role of **Nominated Individual for Data Control**, reporting to the DPO.
- 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. (see Privacy Notice section in the appendix)
- 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.
- 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. (many memory sticks/cards and other mobile devices cannot 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 once it has been transferred or its use is complete.

14. Social Media – Protecting Professional Reputation and Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools 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 liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Linton School provide the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, 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/academy staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school/ academy 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
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- Consent forms are filled in and signed by the pupils parent/guardian

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 may be dealt with under school/academy disciplinary procedures
- Consent forms are filled in and signed by the pupils parent/guardian

Personal Use:

- Personal communications are those made via a personal social media accounts. 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 Head Teacher, and/or the Online Safety Lead, to ensure compliance with the school policies, will check the school's use of social media for professional purposes regularly.

15. Staff using work devices outside of school

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
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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 – Sean Di Sora.

16. 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:
    - 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:

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

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.

17. Monitoring arrangements

This policy will be monitored through scrutiny of risk assessments and records of incidents.

Evaluation will be through discussion with staff and feedback from young people.

The policy will be reviewed at least once a year, or whenever appropriate or necessary to do so. **The next annual review is due in September 2023.**

18. Links to other policies

- Safeguarding & Child Protection Policy;
- Anti-bullying policy;
- Behaviour Policy;
- Health & Safety Policy;
- Risk Assessment Policy;
- Staff Conduct Policy;
- Staff Disciplinary & Grievance Policy;
- Acceptable Use Agreement

Appendix 1: Linton School – Use of computers risk assessment

CareTech Community Services - Risk Assessment

Location: Linton School
Tel: 01772 957062 **Date: 24.09.2022**

Task / Activity	**Risk Rating** (if following the control measures)
Use of school computers and laptops	Medium due to the staffing ratio and structures in place.

Who is at risk from the activity? **(Include all persons including members of staff, people who use our service, visitors, contractors etc).**

Young people, members of the public, staff

What are the hazards (dangers) associated with the task?

Dangers from Internet use without a filter: secure access to inappropriate material on-line; access to websites and apps that are inappropriate for school and for our young people including Chat Rooms and Social Media.

Non-internet use: the computers can be used by any young person so inappropriate content could be left for another young person/staff member to access.

There are no separate areas for file storage so pupils may save files on a computer which could be accessed and tampered with by other pupils.

Pop-up messages sometimes indicate that the anti-virus software is out of date on some computers. It is not possible to update anti-virus software from the school- this has to be done centrally by IT.

There are not enough computers for staff to use these to plan and deliver lessons – as a result teaching staff sometimes use their personal laptops in school.

What are the potential outcomes from the hazards (risks)?

Cyber bullying or on-line grooming (as a victim or perpetrator)

Access to inappropriate material and/or social media platforms

Threats to the school/ company IT systems by malicious intent or by accident (eg hacking into our systems and changing passwords; downloading malicious software or accessing confidential information)

Staff are putting themselves and young people at risk by using their personal laptops in the classroom.

Could any other injuries or incidents occur which are associated with the task or activity?

What actions are taken to reduce the risks? **(Known as control measures)**

- Young people are monitored 1-1 closely supervised throughout whilst on the internet
- Safe Internet and Appropriate Use contract is signed by all young people and staff
- Young people who do not follow this contract will lose their access to IT until it is deemed safe for them to have it again
- E-safety is part of the IT and PSE taught curriculum
- Separate log-ins for staff and pupils: staff do not use these when there are pupils present to reduce the risk of them seeing passwords, or seeing confidential information.
- Staff have completed the Data Protection training

What other actions could be taken, or need to be taken, to further reduce the likelihood of injury. Detail anything specific which needs to be done in the Service? **(Site specific information)**

For any filtering to work properly, the school staff need permission to be able to administer this to unblock sites that we want to access for educational purposes.

Ensure anti-virus protection is updated regularly- senior school staff should have administer rights to ensure they are able to do this

A member of school staff to complete the CEOPS Ambassador training to ensure all staff and students know about risks on-line and what to do to reduce these

Ensure there are enough computers in school for teaching, learning and assessment purposes

What is the likelihood of the risk occurring after control measures have been taken?

HIGH	
MEDIUM	
LOW	X

Who prepared the Risk Assessment and when?

Sean Di Sora, Deputy Head Teacher (ICT Lead)

Who added any “site specific” information as detailed above?

Paul Barton

Who needs to know about the findings of the Risk Assessment?

Declan Tuer, Rebekah Dennett, Paul Barton, school staff, young people

References

https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/

https://www.saferinternet.org.uk/

https://360safe.org.uk/

Appendix 2: Pupil Acceptable Use Agreement

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the ROC Northwest Schools' systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the School's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate, or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school eg. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature: .....

Appendix 3: Staff Acceptable Use Agreement

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet, and other digital information and communications technologies, are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupil*s* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/CareTech newsletter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school's equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or has been agreed in discussion with a senior leader.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School's Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....