Online Safety Policy

September 2024

Contents: **Page no:**

Important contacts 3

Our school, culture, ethos and values 4

1. Aims 5
2. Legislation and guidance 5
3. Introduction 6
4. Roles and Responsibilities 6
5. Educating pupils about online safety 9
6. Allegations of abuse made against other pupils 11
7. Cyber-bullying 16
8. Examining electronic devices 17
9. Responding to incidents of misuse 18
10. Filtering and monitoring 20
11. Mobile technologies (including BYOD) 21
12. Use of video and digital images 23
13. Data protection 24
14. Social media – Protecting professional reputation and identity 25
15. Staff using work devices outside of school 26
16. Training 26
17. Monitoring arrangements 27
18. Links to other policies 27

Appendix 1: Linton School – Use of computers risk assessment 28

Appendix 2: Pupil Acceptable Use Agreement

Appendix 3: Staff Acceptable Use Agreement

Important contacts

ROLE/ORGANISATION	NAME	CONTACT DETAILS
Designated Safeguarding Lead (DSL)	Sean Di Sora	Sean.disora@lintonschool.co.uk 01772 957062 07840 803896
Deputy DSL	Steph White	Steph.white@lintonschool.co.uk 01772 957062 07958 717282
Deputy DSL	Paul Barton	Paul.barton@lintonschool.co.uk 01772 957062
Regional Lead	Declan Tuer	Declan.tuer@caretech-uk.com 07827 302334
Local Authority Designated Officer (LADO) for Lancashire County Council	Tim Booth	Tim.booth@lancashire.gov.uk 01772 536694
Lancashire County Council – Multi-Agency Safeguarding Hub (MASH)		0300 123 6720 0300 123 6722 (out of office hours)
Local Authority Designated Officer (LADO) for Blackpool Council	Amanda Quirke	Amanda.quirke@blackpoo.gov.uk 01253 477541
Blackpool Council – Multi-Agency Safeguarding Hub (MASH)		01253 477299
Channel helpline		020 7340 7264
Prevent / Channel Referrals		concern@lancashire.pnn.police.uk
CAE Service Desk		01923 944399

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 (SEMH) 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

- 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')
- develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, iPads, or 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, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education 2024, 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.

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

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

4.1 The Regional Lead/Proprietor Representative & Head Teacher

The Regional Lead/Proprietor Representative has overall responsibility for monitoring this policy and holding the Head Teacher to account for its implementation.

The Regional Lead/Proprietor Representative should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The Regional Lead/Proprietor Representative and Head Teacher 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 Regional Lead/Proprietor Representative will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

Regional Lead/Proprietor Representative 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 or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with Special Educational Needs (SEN) and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

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

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

4.2 The Designated Safeguarding Lead

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 Head Teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head Teacher and the Regional Lead/Proprietor Representative 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. This is currently monitored by Cambian IT Intranet safety
- Working with the Online Safety Lead to make sure the appropriate systems and processes are in place
- Working with the Head Teacher, Online Safety Lead 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 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
- 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
- Read, understand and help promote the school's Online Safety Policy and procedures.
- Read, understand and adhere to the school Staff Acceptable Use Agreement.

- Be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school procedures with regard to these devices;

- Ensure that any digital communications with pupils are on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones or social media messaging or posts

This list is not intended to be exhaustive.

4.3 Online Safety Lead

The Online Safety Lead 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
- 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.

4.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy having read and understood the policy
- Implementing this policy consistently
- All members of staff will have their own unique username and private passwords to access

  our systems; members of staff are responsible for keeping their password private
- All members of staff are provided with a school Microsoft 365 email address to use for all official school communication. All user school accounts are disabled once the member of the school has left school employment.

- 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
- 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 speaking with the DSL immediately and logging an incident report on Behaviour Watch
- 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'

- Complete the necessary mandatory CPD training on a yearly basis

This list is not intended to be exhaustive.

4.5 Parents/carers

Parents/carers 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

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- www.nspcc.org.uk/keeping-children-safe-online

4.6 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.

Main online safety risks

Online-safety risks are traditionally categorised as one of the **4 Cs: Content, Contact, Conduct** or **Commerce** (see KCSIE). These areas provide a helpful approach to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, and it is important to understand the interplay between all three. This is evident in Ofcom's Media and Attitudes Report 2022 which suggests 36% of children aged 8-17 had seen something 'worrying or nasty' online in the past 12 months, with 84% experiencing bullying via text or messaging, on social media, in online games, through phone or video calls, or via other aps and sites. KCSIE highlights additional risks e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families, including sexual and criminal exploitation, serious youth violence, upskirting and sticky design

6. Allegations of abuse made against other pupils

It is vital that all staff recognise that online-safety is a part of safeguarding. 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 child-on-child abuse. However, all child-on-child 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 Child Protection and Safeguarding 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)

See Linton School's Safeguarding and Child Protection Policy for more details.

6.1 Procedures for dealing with allegations of child-on-child 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. This will include considering school transport as a potentially vulnerable place for a victim or alleged perpetrator(s)
- The DSL will contact the Children and Adolescent Mental Health Services (CAMHS), if appropriate

If the incident is a criminal offence and there are delays in the criminal process, the DSL will work closely with the police (and other agencies as required) while protecting children and/or taking any disciplinary measures against the alleged perpetrator. We will ask the police if we have any questions about the investigation.

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

We recognise the importance of taking proactive action to minimise the risk of child-on-child 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

- Be alert to reports of sexual violence and/or harassment that may point to environmental or systemic problems that could be addressed by updating policies, processes and the curriculum, or could reflect wider issues in the local area that should be shared with safeguarding partners
- Support children who have witnessed sexual violence, especially rape or assault by penetration. We will do all we can to make sure the victim, alleged perpetrator(s) and any witnesses are not bullied or harassed
- Consider intra familial harms and any necessary support for siblings following a report of sexual violence and/or harassment
- Ensure staff are trained to understand:
    - ✓ How to recognise the indicators and signs of child-on-child abuse, and know how to identify it and respond to reports
    - ✓ That even if there are no reports of child-on-child 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 child-on-child 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
    - ✓ That social media is likely to play a role in the fall-out from any incident or alleged incident, including for potential contact between the victim, alleged perpetrator(s) and friends from either side

The DSL will take the lead role in any disciplining of the alleged perpetrator(s). We will provide support at the same time as implementing sanctions.

Sanctions can be implemented while other investigations are going on, e.g. by the Police. The fact that another body is investigating or has investigated an incident doesn't (in itself) prevent our school from coming to its own conclusion about what happened and imposing a penalty accordingly. We will consider these matters on a case-by-case basis, taking into account whether:

- Taking action would prejudice an investigation and/or subsequent prosecution – we will liaise with the Police and/or LA children's social care to determine this
- There are circumstances that make it unreasonable or irrational for us to reach our own view about what happened while an independent investigation is ongoing

6.3 Sharing of nudes and semi-nudes ('sexting')

This guidance is based upon guidance from the UK Council for Internet Safety for all staff and for DSLs and senior leaders.

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.

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 headteacher 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/carers
The DSL will inform parents/carers 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 the local neighbourhood police, dialing 101.

Recording incidents
All incidents of sharing of nudes and semi-nudes, and the decisions made in responding to them, will be recorded. The record-keeping arrangements set out in this policy also apply to recording these incidents.

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

This policy on the sharing of nudes and semi-nudes is also shared with pupils so they are aware of the processes the school will follow in the event of an incident.

6.4 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.

Young People Under the Age of 13
Under the Sexual Offences Act 2003, children under the age of 13 are considered of insufficient age to give consent to sexual activity. The Police must be notified as soon as possible when a criminal offence has been committed or is suspected of having been committed against a child unless there are exceptional reasons not to do so.

Young People Between 13 and 16
The Sexual Offences Act 2003 recognises that whilst mutually agreed, non-exploitative sexual activity between teenagers does take place and that often no harm comes from it, the age of consent remains at 16. This acknowledges that this group of young people are still vulnerable, even when they do not view themselves as such.

Young People Between 16 and 18
Although sexual activity in itself is no longer an offence over the age of 16, young people under the age of 18 are still offered protection under the Children Act 1989.

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.

6.5 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 'Recognising abuse and taking action' section in this document. 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).

6.6 Reporting systems for our pupils

Where there is a safeguarding concern, we will take the child's wishes and feelings into account when determining what action to take and what services to provide.

We recognise the importance of ensuring pupils feel safe and comfortable to come forward and report any concerns and/or allegations.

To achieve this, we will:

- Put systems in place for pupils to confidently report abuse
- Ensure our reporting systems are well promoted, easily understood and easily accessible for pupils
- Make it clear to pupils that their concerns will be taken seriously, and that they can safely express their views and give feedback

7. Cyber-Bullying

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 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.

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 or Speech and Language Therapists.
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.

Reporting Incidents of Cyberbullying

- Speak to the DSL or Deputy DSL and inform them in the incident of cyberbullying
- Record the incident on Behaviour Watch
- The DSL or Deputy DSL will look at the incident and decide how to respond by using the Anti-bullying, Safeguarding and Child protection and Behaviour policy to support any decisions made

Please see Linton School's Anti-Bullying, Behaviour and Online Safety 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:

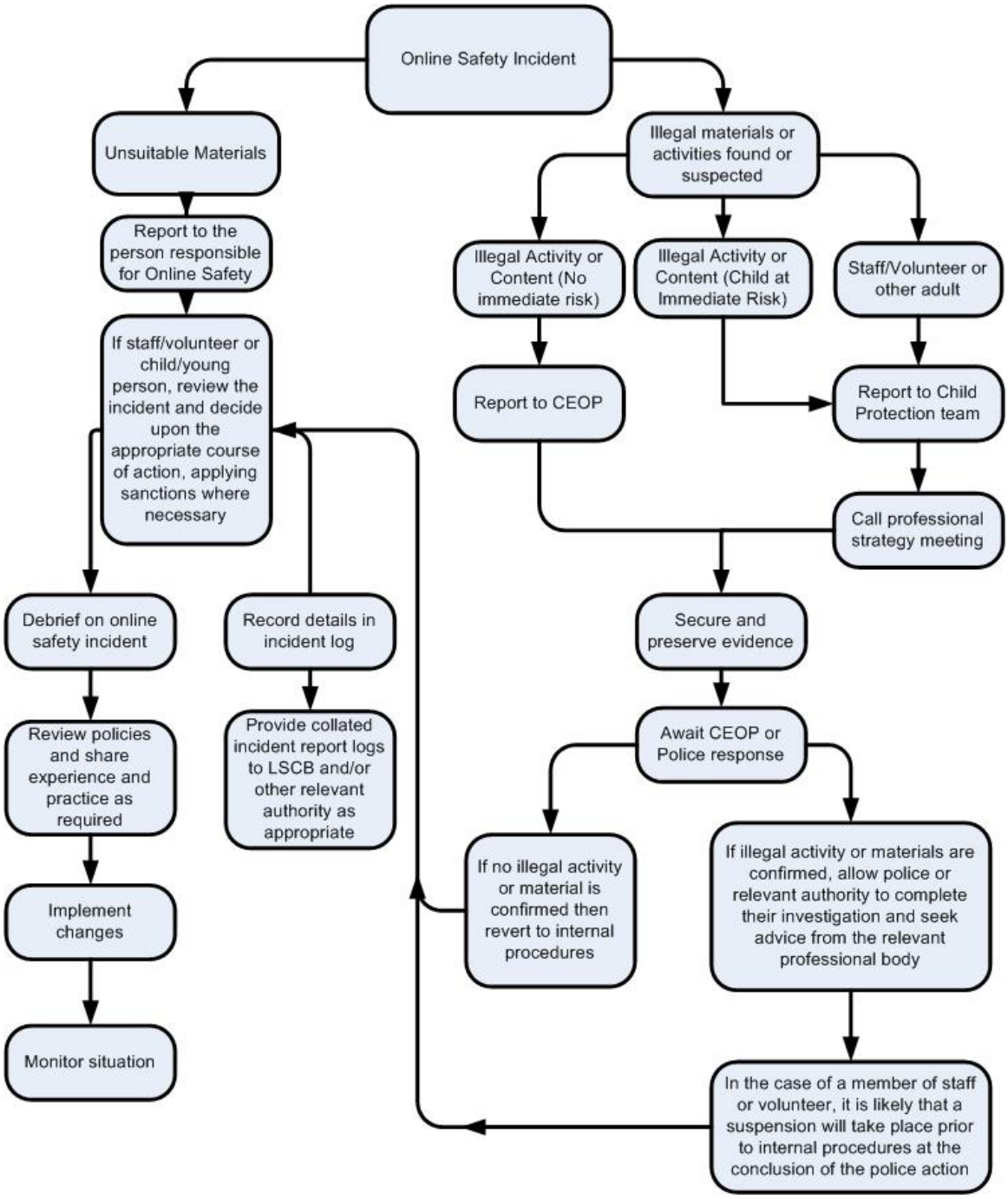
- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

Linton school 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. Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

Additionally, schools will need to liaise and communicate effectively with CareTech/Cambian 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/Cambian 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 and this is by raising a ticket with the CAE Service Desk that all staff have access to on their laptops, alternatively staff can call 01923 944399.
- 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).

Reporting concerns regarding to filtering and monitoring

- Staff should speak to the DSL or deputy immediately
- Log their concerns on Behaviour Watch
- The DSL or deputy must call the CAE Service Desk on 01923 944399 open a new ticket and log it as a safeguarding concern
- From there the CAE Service Desk will work with the DSL or deputy and next steps can be established

For making changes or getting websites reviewed

- Staff should speak to the DSL or deputy immediately
- The DSL or deputy must call the CAE Service Desk on 01923 944399 open a new ticket
- From there the CAE Service Desk will work with the DSL or deputy and next steps can be established
-

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
- 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 CareTech/Cambian IT Department.
- Technical support is provided by CareTech/Cambian IT Support Services
- Filtering of devices is administered by CareTech/Cambian IT Support Services
- 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.

Mobile phones/devices

- Pupils are allowed mobile phones/devices for transport purposes only and only those pupils who are arriving in Local Authority provided transport.
- All pupils arriving to school in transport provided by Linton School should not have mobile phones or devices and these should be left at home.
- When a mobile phone/device is needed to be brought into school the parents or carers should inform the school teaching staff as soon as possible.
- Where a parent or carer suspects that a child or young person has a phone on them then this should be reported to school teaching staff as soon as possible.
- Any mobiles phones/devices being brought on to school property should be handed into the school office at the start of the day and should be collected as that person is leaving school to access their transport home.
- In cases, where a mobile phone/device causes an issue to the learning or welfare of students then this device will be confiscated. On the first occasion this device will be returned to the student at the end of that day. From the second occasion onwards the parent/carer would need to collect that device from the school office.
- For persistent violations of the school rules regarding mobile phones/devices then a weeks ban will be placed and the school would require parent/carer support to enforce this.

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:

All staff and students must sign the Acceptable Use of ICT agreement.

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 (DSL or Deputy DSL) – 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.
- Emails being sent to external parties must be sent using Egress.

All staff and students will sign the 'Acceptable Use of IT agreement' in recognition of the above terms.

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, as in acted by the UK's Data Protection Act 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 Company fully endorses and adheres to the six principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. The Company will retain its data and records in accordance with the requirements of ISO 9001/2008 and other appropriate Regulations and Standards.

The Data Protection Principles
The principles require that personal information must be:

a. Processed lawfully, fairly and in a transparent manner;
b. Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes;
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d. Accurate and, where necessary, kept up to date;
e. Not kept in a form which permits identification of individuals for longer than necessary, in relation to the purposes for which it is processed;
f. Kept secure, and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Company have appointed a Data Protection Officer who is ultimately responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Information Governance Board. Any questions or concerns about the interpretation or operation of this policy should be taken up, in the first instance, with the Data Protection Officer who can be contacted at: Data.Protection@CareTech-UK.Com

Notifying the Data Protection Officer of certain activities
A Data Protection Impact Assessment must be undertaken prior to undertaking certain activities that involve processing personal information.

A 'data protection impact assessment' will consider the impact of the activities on individuals; identify privacy risks and steps to minimise those risks; and evaluate whether the activities are permitted by data protection law.

Employees should seek advice from the Data Protection Officer so they can advise whether a data protection impact assessment is required in the following situations:

a. Process new types of personal information i.e. personal information which has not been collected before.
b. Process personal information in a new or significantly different way, including via the use of new technologies.
c. Use personal information for a purpose other than that for which it was collected.
d. Enter a contract with a third party that involves disclosing or sharing personal information.
e. Any new or significantly different use of automated processing of personal information to evaluate an individual, for example to analyse or predict an individual's performance at work, health, personal preferences, interests, reliability, behaviour, location or movements.
f. Any new or significantly different use of automated decision-making i.e. where a decision is made on a solely automated basis without meaningful human involvement, and it has a significant effect on individuals.

g. Any new or significantly different large-scale processing of special categories of personal information; or large scale, systematic monitoring of a publicly accessible area. Whether processing is 'large scale' will depend on, for example, the number of individuals, volume of data, range of data, duration of processing, or geographical extent – if you are in any doubt as to whether processing is large scale, contact the Data Protection Officer.
h. Implement significant changes to systems or the business (including new or different technology) which involve processing personal information.
i. Any direct marketing activity to individuals (including electronic marketing by email, telephone, fax or text message).
j. Transmit or send personal information to, or view or access personal information in, a country outside of the United Kingdom or the EEA where this has not been previously authorised by the Data Protection Officer or in line with the Group's Data Protection Policy. The EEA is the 28 countries in the European Union, along with Iceland, Liechtenstein and Norway.

Employees must comply with any directions from the Data Protection Officer in relation to the above, and the terms of any data protection impact assessment.

Please see the company's Data Protection Policy available at Linton School Preston - Special needs school for young people for more information.

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 staff should ensure that:

- No reference should be made in social media to pupils, 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
- 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

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
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.

Staff will not use personal devices:

To take photos or videos of learners and will only use work-provided equipment for this purpose unless specific permission has been given by the Headteacher.

If staff have any concerns over the security of their device, they must seek advice from the Online Safety Lead – 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).

Staff will access the NSPCC / CEOP's materials to support the effective delivery of Online Safety across the school.

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.

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 2025.**

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
- Data Protection

Appendix 1: Linton School – Use of computers risk assessment

CareTech Community Services - Risk Assessment

Location: Linton School
Tel: 01772 957062 **Date: 18.09.2024**

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, Head Teacher

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

Paul Barton

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

Declan Tuer, Andy Cavill, Tracey Pinder, 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 Caretech 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 pupils 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 the Regional Lead/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: .....