The Lioncare School Policy for Online Safety 2021-2022

Policy Type and Title	Related Documents	Related Legislation	Author	Consultation	Curriculum Links	Date Created	Date for review
The Online Safety Policy This is a Safeguarding Policy	Safeguarding and Child Protection Guide to Safe Working Practices Employee Handbook Record management Policy Risk Assessment Policy Policy for Promoting Positive Behaviours and Relationships Health and Safety Policy	The Independent School Regulations 2015 and 2018 amendment Keeping Children Safe in Education (DfE 2021) Working Together to Safeguard children (DfE 2018)	Sara Fletcher Caroline Belchem	The adult team at The Lioncare School The Lioncare School Safeguarding Consultant (Beccie Mannall) The Lioncare Group Safeguarding Monitoring Group	Computing Keeping Safe Global Communities	Created 08/13 Reviewed: by SF and school team: August 14 August 15 August 16 August 17 April 18 August 19 August 20 (MS AA SF TM)	August 22

						July 21 CB	

Introduction

The purpose of ICT and Internet use in school is to raise educational standards, to promote participation in wider communities, to support the professional work of staff and to enhance the school's management functions. The Lioncare School recognises that Information and Computing Technologies and the Internet are significant tools for learning and communication that can be used in school to enhance the curriculum, support creativity and foster independence. A proactive engagement with the opportunities for personalised and differentiated learning, and connectivity with a range of communities can be transformative for all learners in school - be they adults or children. However, access to ICT equipment and to the Internet must be viewed as a responsibility; and systems in place that ensure everybody uses them appropriately and practices good online safety.

It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online. We use the term "online safety" rather than e-safety or cyber safety to ensure the emphasis is on maintaining standards of behaviour and attitudes that are sustainable and transferable across settings rather than tied to thinking about technology or equipment. Any risks are as a result of poor or ill-informed choices rather than related to the technology itself. Online safety covers the Internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings. There is a 'duty of care' for any person working with children and educating all members of the school community on the risks and responsibilities of online safety falls under this duty. We also recognise that there are other risks online to children that include the risk of radicalisation from extremist groups, identity theft, and the risk of criminalization from their own behaviour. In addition, the complex family networks of the children at the Lioncare School mean that there is an extra dimension of risk from contact from those who may seek to deliberately harm them or with whom any contact may cause distress and anxiety. This policy also makes it clear that the adults in school have a responsibility not only to supervise, support and educate children and young people but to manage their own online presence and activities responsibly in and out of the school building as well. Online safety is a whole-school issue and responsibility, and this includes visitors to the school. Online bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures, which are outlined in our **Policy for Promoting Positive Behaviours and Relationships.**

Contents

1. Responsibilities
2. A Child Centred Community
3. Online Risks
4. Online Safety Agreement
5. Safer Internet Day
6. ICT for learning and curriculum links

7. Young people and social media
8. Young people and personal devices
9. Sexting
10. Online bullying
11. Supervision and monitoring (blocking and filtering)
12. Emergent technology and content
13. Images/video recording
14. Adult safe use and online conduct
15. Adult use of email
16. Visitors to the school
17. Management Information Systems
18. Training, development and professional support
19. System Security
20. Personal Data
21. Published Content
22. Sources of support and information

Responsibilities

This Policy Applies to:

- All those directly employed by The Lioncare School and who are in positions and roles that require them to interact with or work alongside or in proximity to the children in our care and receiving an education from us.
- All those indirectly employed by The Lioncare School by being commissioned and paid to undertake work alongside or in proximity to the children in our care and receiving an education from us (i.e. engaged in regulated activities)
- Others working in partnership with The Lioncare School in regulated or unregulated activities, whether paid or not, who work alongside or in proximity to the and receiving an education from us.
- Visitors to our school

Responsibilities:

All employees, whether they have a "front-line" role directly engaged with the care and education of children (teachers, learning support assistants, adults in school) or "ancillary" (e.g. maintenance worker, housekeeper/cleaner, administrator) are personally responsible for managing their own conduct in relation to all aspects of safeguarding and child protection, including working to the standards set out in this policy. All employees are also responsible for supporting their colleagues, as well

as visitors to the school to follow this policy at all times. All adults employed by the school are required to be familiar with this policy and those linked to it, with our Guide to Safer Working Practices and with Keeping Children Safe In Education (2020) In additional all adults should be aware that we work along within the Pan-Sussex Safeguarding and Child Protection Procedureshttp://sussexchild protection. procedures.org.uk/.
Visitors will be provided with summary information relevant to their task in school.
Sara Fletcher is the Assistant Director For Education and Learning and Designated Safeguarding Lead of the Lioncare School and as such has a duty of care for ensuring the safety (including online safety) of members of the school community, Sara is supported by Caroline Belchem Head Teacher and Deputy Designated Safeguarding Lead, and Zena Maher the online safety coordinator.
The Head Teacher must:
Ensure access to induction and training in online safety practices for all users.
Ensure appropriate action is taken in all cases of misuse.
Ensure that Internet filtering methods are appropriate, effective and reasonable.
Ensure that staff or external providers who operate monitoring procedures are supervised by a named member of staff.
Ensure that pupil or staff personal data as recorded within the school management system or sent over the Internet is managed securely.
Work in partnership with the DFE and the Internet Service Provider and online safety coordinator to ensure systems to protect students are reviewed and improved.
Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

The Online Safety Coordinator must:
Work in partnership with the DFE and the Internet Service Provider and Head Teacher to ensure systems to protect students are reviewed and improved.
Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
Report to senior colleagues as required.
Ensure, in partnership with the head teacher and the organization’s ICT consultant, that the school’s technical infrastructure is secure and is not open to misuse or malicious attack.
Ensure, in partnership with the head teacher and the organisation's ICT consultant, that the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.
Ensure, in partnership with the head teacher and the organisation's ICT consultant, that users may only access the networks and devices through a properly enforced password protection policy.
Ensure, in partnership with the head teacher and the organisation's ICT consultant, that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
Ensure, in partnership with the head teacher and the organisation's ICT consultant, that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

It is the responsibility of all staff to know when an online issue has become a child protection concern and report this concern to the Designated Safeguarding Lead (Sara Fletcher) and/or Deputy Designated Safeguarding Lead (Caroline Belchem) as outlined in The Lioncare School Safeguarding and Child Protection Policy. It is the responsibility of the DSL/DDSL to log all such incidents for the scrutiny of the organisation's Safeguarding Monitoring Group.
For 2021/22 the role of “On-line safety coordinator” is shared by the school administration team

A Child Centred Community

Central to the therapeutic education model practiced at the Lioncare School is the belief that an individual child can only have damage from their earliest years addressed in a setting that allows for relatedness to others. Our practice is based on Psychosocial Theory, influenced by Group Relations thinking, informed by the work of Klein, Winnicott, Bion, Bowlby, and Hinshelwood amongst others. In this way, the model used at The Lioncare School resembles the Therapeutic Community Approach'. The idea at the heart of the model is one of equality between people and of the capacity in each of us to help and heal each other and to contribute to each other's development. It emphasises the quality of communication between adults and children (and between the adults), and on the connections between the help provided to individuals and the overall task with the whole group. Therefore, the key areas we are constantly attempting to nurture in the children at The Lioncare School (and the adults working with them) is the ability to be honest, open and reliable with each other, and willing to find ways to communicate difficulties and problems more effectively and to begin to take responsibility for their own actions, decisions and lives. It is our firm belief that our Therapeutic Curriculum based on the following five principles is a protective mechanism for keeping our children and young people safe both in school and over their journey to interdependence.
Attachment: Children and young people attending The Lioncare School need to feel a healthy sense of belonging. They are encouraged to become full members of a group that values them and gives them something to value. This is a fundamental first step in the feeling of self-worth necessary for learning to begin and it also means that they will not accept being treated badly by others and will speak up for themselves, trusting others to hear them. They will begin to accept that a reliable adult can hear about unpleasant experiences without blaming or rejecting the child. The low self-worth will contribute to risk taking behaviours online and a vulnerability to those who use the internet to exploit others. All adults should be aware that traumatized children are more vulnerable than their chronological peers.
Containment: Safety is paramount for our children and young people. All children and young people have a need to experience an appropriate degree of consistency, predictability, and regularity in their daily lives, and it is this that promotes a child or young person's sense of being 'safe' and is a prerequisite for children and young people developing the ability to retain new facts and skills (i.e. 'learning'). Our children and young people have often had limited experience of this. When the child recognises what feeling safe is like they can begin to identify those things that were and are not safe and begin to want to protect themselves in healthy ways. This includes children and young people understanding that adults will uphold all boundaries around online usage.
Communication: Children at The Lioncare School need to see that openness is important in moving forward and that the adults can work honestly and respectfully with everything they need to communicate. In school this means teaching socially appropriate communication is more successful when adults show they can understand and manage less positive communication. Our children have often had early experiences that have deprived them of knowledge of the wider world and

of different communities and therefore online worlds can be enriching and reparative in these areas but all adults must be aware children and young people need to be taught the conventions of online communication in order to stay safe.
Involvement: The children and young people attending The Lioncare School learn about "growing-up" by experiencing the interdependency of participation in individual and group learning. In school this means a number of different activities are planned each week to give new experiences at the right level for each child; these can be very small step achievements, but by finding value in them self-worth grows and the capacity to assert choice. Adults must stay attuned to when online activity is an enhancement to this or used by a young person to defend against involvement,
Agency: Agency can be defined as the acquiring of skills, actions, medium, or means by which to accomplish things. As children and young people move through the school they grow closer to taking control of their lives and learning post-16 and need to experience both success and failure to do so. This also means that as children and young people progress through the school they are actively encouraged to take up roles and positions of increasing responsibility and authority through making and evaluating decisions. This means greater online autonomy can be planned for as young people reach the capacity to manage this and adults are clear on how they will be able to evaluate the success of any such steps.
We believe this ethos, in partnership with the robust procedures detailed below and in other policies, informs an environment where children learn to keep themselves safe, demand safety from others and in which adults are attuned to how to work safely and how to spot the earliest possible indicators that things are not safe. Children learn to recognise and manage risks in different situations and then decide how to behave responsibly, judge what kind of contact is acceptable and unacceptable and recognise when pressure from others (including people they know) threatens their personal safety and wellbeing and develop effective ways of resisting pressure. These skills are meaningful online and in real life.

Acknowledgment is duly given to the work of Adrian Ward, Senior Lecturer in the department of social work at the Tavistock and Portman NHS Foundation Trust. 5 2 Haigh, R. (2013) "The quintessence of a therapeutic environment", Therapeutic Communities: The International Journal of Therapeutic Communities, Vol. 34 Iss: 1, pp.6 -15

Online Risks

The Lioncare School works with children and young people in Key stages Two, Three and Four who have experienced abuse and neglect in their early years and often much disruption due to multiple placement breakdowns. In many cases children and young people often have diagnosed cognitive, neurological or communicative disorders. We assess that these children and young people are vulnerable to all or some the following risks while online or while using ICT equipment, individual risks are outlined in Safeguarding Risk Profiles and managed through Positive behaviour Support Plans:

1. Unplanned contact with an unsafe adult known to them who may mean then harm
2. Unplanned contact with an unsafe adult known to them who may not mean them harm but who may unintentionally cause emotional distress
3. Unplanned contact with an adult unknown to the child who intends to harm them or entice them into harmful behaviour
4. Engaging in harmful or exploitative sexual behaviours
5. Becoming the victim of online bullying by those known to them

6. Becoming the victim of online bullying by those unknown to them
7. Being rejected by friendship groups due to immature social skills
8. Sexting: receiving inappropriate images
9. Sexting: sending inappropriate images and risking criminalization
10. Invasion of privacy
11. Identity theft
12. Theft through fraudulent payment systems or scams online
13. Theft through insecure password protection
14. Being hacked and losing control of personal data
15. Leaving personal information on devices which are sold or swapped
16. Excessive spending on "in app" and gaming purchases
17. Criminalization through intentional/unintentional illegal downloading/file sharing
18. Exposure to inappropriate images, including those that lead to distressing thoughts (and increased potential for self-harm)
19. Exposure to triggering images that lead to distressing thoughts (and increased potential for self-harm)
20. Exposure to, and possible desensitisation, to physical violence
21. Exposure to, and possible desensitisation, to sexual violence
22. Anxiety due to worrying news stories
23. Opportunity to shop for harmful or illegal items
24. Radicalisation by extremist groups both in the UK and abroad
25. Introduction to gang culture
26. Isolation from groups in real life
27. Limitations on experiential learning and physical activity
28. Physical harm from poor posture or over exposure to screen
29. Physical harm from poor sleep
30. Sensory overload
31. Damage to equipment due to downloading malware or spyware
32. Theft of personal devices
33. Exposure to unhealthy lifestyle sites such as "ProAna" forums and those promoting self-harm
34. Learning about dangerous fads such as those that involve ingesting harmful substance
35. Temptation to join "daredevil" or "pranking " competitions leading to harm or arrest
36. Developing issues around body confidence due to unrealistic images
37. Damaged reputation and reduced job opportunities

We believe that the best protective factors are alert, attuned and knowledgeable adults, confident young people equipped to make good choices, a positive and open community and secure technological equipment.

Our On-line safety agreement

At the beginning of each term every class revises the agreement below and places a poster sized version on the wall. This is signed by all users. Individuals may be asked to resign the agreement if they have lost the right to use ICT equipment for any time.

We respect our equipment by:	**We respect our classmates by:**	**We respect our adults by:**	**We respect our health by:**
Remembering it is here to help us learn Using it in ways that adults have said is OK Keeping food and drink away from it Not throwing it, pushing it off the desk, hitting it or throwing things at it Tidying away properly	Looking after equipment Sharing equipment Coming off equipment when asked by an adult Coming off of equipment when asked by an adult Coming off equipment for group activities without being asked Not playing loud or offensive videos or music Not putting upsetting pictures on equipment Not filming or taking pictures of each other	Using all equipment at agreed times only Showing that we know computers are for learning Coming off computers when asked or when we know we should Stopping any on-line activity when we are asked to or closing a screen when we are asked to Not trying to hide what we are doing Remembering the adults are here to help us learn and keep us safe	Not using a computer or any screen for more than thirty minutes at a time Not using headphones on high volume or for longer than 30 minutes (for our ears) Sitting in a proper chair at the right height for our backs Sitting up with the mouse and keyboard and screen in the right place (for our arms, wrists and shoulders) Washing our hands before we use a machine or device and wiping it clean afterwards

I respect myself by: Signing the school's online safety guidelines in my classroom so I can learn safely Letting myself use technology to learn new and interesting skills and ideas including Safer Internet Day Being a responsible user of the school's systems and equipment. If I can not be responsible I understand I'll need time away from the equipment. Keeping my personal information personal and never sharing it Not breaking the laws on hacking accounts, sending threatening and offensive messages, inappropriate pictures or trying to download music, films or games at school Knowing that people online are not always who they say they are and I can't trust them Not using technology to be unkind to people Not searching for things that make me feel worried or upset Not playing violent games or accessing other content not appropriate for children Speaking to an adult I trust if anything happens online which makes me feel uncomfortable or worried Letting adults keep the portable devices safe			

Safer Internet Day

The Lioncare School encourages a whole community approach to Safer Internet Day each February by choosing a theme and sharing activities and resources across school and home. Previous themes have included online "stranger danger", protecting identity and safer gaming. In 2021 Safer Internet Day is on February 9th and

we will be using the week to explore online relationships, how to spot risks and report them and the responsibility to be responsible and respectful on-line, as in "real" life, at all times.

ICT for Learning and Curriculum Links

Our curriculum model (C2020) is based on fostering the key skills that we wish all young people to have at the end of their education with us, whether this be after key stage four or earlier. We do indeed want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school, however we see it as equally important that they learn to have an online presence that is safe and included, that they are informed and empowered citizens, protected consumers and entertained audiences for cultural media.
Our key performance indicators for Computing are:

I can recognise ways to use ICT in my learning.
I can recognise ways ICT is used beyond school.
I understand computer networks and how they provide opportunities for communication and collaboration
I can use technology safely, respectfully and responsibly
I can use technology to create, organize, retrieve and find things
I can understand how searches work and evaluate what I find
I can use technology to present information to others

And all teachers have a responsibility to embed these skills into all aspects of our Project Based Learning Model.

Over 2020-21 we will be adding tasks, including around Safer Internet day that provide evidence of progress under the new Relationship, Health (and Sex) education curriculum, and integrating this into C2020
The outcomes for this are:

By age 11 Children will know	By age 16 Children will know
1. that people sometimes behave differently online, including by pretending to be someone they are not 2. 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. 3. the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.	1. their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online. 2. 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.

4. how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met. 5. how information and data is shared and used online.	3. not to provide material to others that they would not want shared further and not to share personal material which is sent to them. 4. what to do and where to get support to report material or manage issues online. 5. the impact of viewing harmful content 6. 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 7. that sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail. 8. how information and data is generated, collected, shared and used online.

Young People and Personal Devices

Personal Devices are not permitted into school unless a child who travels to school independently has been assessed as needing one for the journey. In such a case a risk assessment will be carried out for most children, most of the time this will mean that the device is kept in the school administration office during the school day. School Wi-Fi codes are not to be given to young people or put on devices. Very occasionally younger children may bring a device in for a longer journey and such devices are not to be connected to the school Wi-Fi.

"Sexting"

Sexting involves sending sexually explicit messages and images, often but not exclusively "naked selfies". A more helpful term is "Youth produced sexual imagery", this helps balance out issues of potential criminality with those regarding positive behaviour, relationships and conduct. There can be a coercive aspect to this communication and the sharing of such images can be a type of "Revenge porn". Being coerced into taking or sharing images and have personal, intimate photos shared is extremely damaging emotionally. All young people need to be made aware that taking, making (including downloading), possessing, sharing, showing and distributing such images is illegal. Coercive behaviour around intimate images is likely to lead to a disruptions process (see Admissions and Exclusions process). Adults need to be aware **they must never look at, download, save or in any way store any image or message. Where possible the device itself needs to be safely stored and given to the police.**

Full guidance is available at
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759007/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf
Any adult that suspects sexting has occurred or might occur must inform the DSL/DDSL and this will become a safeguarding issue and reported and recorded under the procedures laid out in the Child Protection and Safeguarding Policy

Online Bullying

The Lioncare School considers online bullying to share the intentions, regularity and same power dynamic as other forms of bullying and as such it is defined by the content of the behaviour and emotional impact on the victim rather than the technology involved. Therefore procedures for managing incidents of online bullying between children at the school are covered in our Policy for promoting Positive Behaviour and Relationships. Where necessary work will involve adults from the Lioncare Group's Therapeutic Children's Homes to resolve issues arising from out of school hours. If an incident of online bullying were to arise involving others from out of school the Head Teacher would consult with the social worker/parents/residential staff of the child involved to decide on an effective strategy unless there was evidence of a child protection issues in which case the procedures outlined in the school's Safeguarding and Child Protection Policy would be followed.

Filtering and Blocking

Adults at The Lioncare School directly supervise young people who are using school computers/tablets, and will actively challenge unsafe use of technology with the young person. As an additional failsafe, all network access is filtered through Netsweeper, a proxy-based web filter which intercepts and blocks any unsafe or harmful content before it reaches the school's network. This ensures a secondary layer of security and online safety alongside the work done by supervising adults in the moment.
The following specific categories and subcategories of content are blocked by Netsweeper for all users at The Lioncare School, including those outlined in the PREVENT duty:

Safe Search
UK Prevent:
Criminal Skills
Extreme
Hate Speech
Weapons
Pornography
Child Pornography
Child Erotica
Suicide

Self-harm

No web filter can be completely robust enough to block all unsafe or inappropriate content from being accessed. It is therefore important not to rely solely on the filter without the active supervision of adults to prevent such content being accessed in the first place, and to challenge/discuss any inappropriate content if accessed or if a young person attempts to access such material. This also ensures proactive learning of online safety is embedded as the first step to keeping safe online. Conversely, no web filter can be trusted not to mistakenly block harmless web content. All senior staff and teachers are provided with logins and instructions on how to use the management system provided by Netsweeper in order to whitelist specific websites which are blocked in error, and to block specific websites which should not be accessible. The online safety coordinator administers the Netsweeper management system, and both School Administrators are able to block and whitelist particular websites on request from adults who do not have Netsweeper accounts.
The web filter generates a weekly report with a list of all blocked websites for which access had been attempted that week. These reports are logged on the school's Google Drive in the Safeguarding subfolder by the online safety coordinator. The online safety coordinator will check each result and comment on the report whether it is a "false positive" or a genuine cause for concern, in which case they will inform the Head Teacher with details of the site and when it was accessed. The Head Teacher will respond appropriately to any concerning reports; this may include seeking advice from the police, local safeguarding networks or other agencies.

Emergent Technology and Content

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies, in part due to updates via newsletters and networking opportunities from the LSCPB and Education Safeguarding Network and newsletters from NASS (National Association of Special School) and the NSPCC, and is prepared to quickly develop appropriate strategies for dealing with new technological developments

Images and Recordings

Photographs have many important and positive uses at The Lioncare School. At times they can provide very strong evidence of achievement for young people who find writing hard and thus give a solid boost to self-esteem. They are also essential in forming new and positive memories for young people who may have very little sense of their life story before their time at school. However, while images are regularly used for very positive purposes adults need to be aware of the potential risks around these. Any image can be taken and/or misused or manipulated for pornographic or 'grooming' purposes. The very act of taking overtly “innocent” photographs of sexually abused children can be harmful if done without sensitivity and consent.
Every step should be taken therefore to ensure that images do not fall into the wrong hands, that no child or young person is distressed by an act of image making and that no adult is put at risk of false allegation by being asked to take or store images in a way that is not safe.
On admission those with parental authority are asked to give permission for images to be taken, but it is clear no image showing a child’s face or identifying features is ever shared publicly for any reason.

On occasion images are shared with examination boards (NCFE, ASDAN, Cambridge) for the purpose of accreditation. Ideally moderation happens in school, if not photographs are taken as hard copies in files, rendered difficult to copy and returned to school after moderation. If this is not possible, it is for the Examinations Officer and the Online Safety Coordinator to scrutinise the examination arrangements and risk assess the safest way to share the images, including the use of secure email systems such as Egress or Voltage as appropriate.
The only place that photographic or video images of children and young people should be stored is on the secure, encrypted, shared Google drive in the folder labelled for this purpose. To be clear the appropriate folders are:

- Children's Individual Folders
- Photos From across the Lioncare Group (Main Shared Drive) No other folders or areas should be used.

Individual image files should not be named in a way that identifies the child. Photographs necessary for identifying children to the emergency services can be stored on Behaviour Watch, the school's management information system.

No adult should have photographs or videos on their personal devices-there are cameras and tablets available in school for gathering photographic evidence of curriculum activities and participation and these should be used where possible. Photographs and videos should be removed from portable devices and uploaded to the named folder at the earliest opportunity. Adults should be alert to members of the public who may take images of children. Adults should always question why they are taking a picture and to what use it will be put and sensitive to the response of children to having their picture taken. If necessary members of the public should be informed the school will consider informing the police if adults suspect images of children are being taken.
Adults should not allow children to film or photograph each other or members of the adult team on their own devices or on school devices without the planned support of an adult as part of a learning task. Adults may need to consider the confiscation of devices if young people cannot follow this guideline. Older children need to be informed they are breaking the law, and risk criminalization, or consequences in school such as loss of ICT/device use.
Children must be asked for their consent for images to be taken. Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that children and young people are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, PE activities), will focus more on the sport than the individual. Children and young people are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in. Injuries to children or young people should not be photographed unless permission has been sought from the DSL and a notification to external agencies is in place. These photos should never be of intimate areas. It is never appropriate to take a photograph of a child or young person who is subject to restrictive physical intervention, distressed or dissociated.
Adults should take extreme care to ensure that children and young people are not exposed, through any medium, to inappropriate or indecent images. There are no circumstances that will justify adults: making, downloading, possessing or distributing indecent images or pseudo-images of children (child abuse images). Accessing these images, whether using the settings or personal equipment, on or off the premises, or making, storing or disseminating such material is illegal. If indecent images of children are discovered at the establishment or on the school or setting's equipment an immediate referral should be made to the Designated Officer (DO) and the police contacted if relevant. The images/equipment should be secured and there should be no attempt to view or delete the images as this could jeopardise necessary criminal action. If the images are of children known to the school, a referral should also be made to children's social care in line with local arrangements.
Under no circumstances should any adult use school or setting equipment to access pornography. Equipment containing pornography or links to it should never be

brought into or used in the workplace. This will raise serious concerns about the suitability of the adult to continue working with children and young people. Staff should keep their passwords confidential and not allow unauthorised access to equipment. In the event of any indecent images of children or unsuitable material being discovered on a device the equipment should not be tampered with in any way. It should be secured and isolated from the network, and the DSL contacted without delay. Adults should not attempt to investigate the matter or evaluate the material themselves as this may lead to a contamination of evidence and a possibility they will be at risk of prosecution. These guidelines are the same if a child is thought to have inappropriate images on their own device. Aligned to this all adults must make sure that any films, music videos and gaming imagery shown in school are age appropriate whatever their own practice at home - to ignore this advice is to risk an allegation of exposing children to images of a sexual nature.

Adult Safe Use

Adults have access to ICT in the workplace to aid their professional task of teaching and supporting children and young people, creating appropriate logs and reports and communicating effectively with colleagues and for other functions associated with their role.
The organisation does not permit adults to use the organisation's equipment to access social media, gaming and gambling sites, or to download any media for personal use. Adults must use all devices safely-this means not sharing passwords either for the network, the google drive or for BehaviourWatch, Shared passwords, i.e. for the handovers file must be updated/changed monthly or at the instruction of a senior team member. Adults must log out of devices and ensure their sleep and other security functions are set appropriately.
Adults may have their own devices on their person in school but must ensure they take responsibility for the safety of these devices, the security of their data and should not allow young people to use devices belonging to adults. Adults should be aware that if they use their own devices to access the Lioncare School Wi-Fi network their activity may be subject to scrutiny via the filtering systems (see Filtering and Blocking). If an adult is seen spending time on a personal device when they should be supervising or interacting with children and young people then disciplinary proceedings may be considered.
Online reputation and conduct
Adults need to be responsible for managing their online presence even when they log on to social media sites out of work time. Adults should:

- Never publicly identify themselves as working for the organisation or make reference to the organisation in any way on social media or any other forum not directly related to work.
- Never bring the organisation into disrepute
- Discuss their work in a way that identifies the organization, colleagues or individual children
- Always be aware of the professional standards for their role as teachers and / or members of the childrens' workforce. This could mean that posts made of social media not directly related to one's working life are at risk of being reported to Safeguarding authorities by members of the public if they are felt to compromise the adult's capacity to safeguard children. This could lead to internal investigation or referral to another agency, including the police.
- Not use work emails to register for any non-work-related site or activity
- Use the highest possible privacy settings online

- Never interact with children and young people or their families online.

WhatsApp

There is a school team WhatsApp group that has three primary tasks:

- For adults on trips and activities to communicate with each other and with school
- For adults across the building to request urgent support with incidents of violence and aggression
- For the team to share information essential to the well-being of children

And a secondary task of supporting safeguarding leads and administrators keep a timeline of critical events. Communications outside of these purposes should be limited. Children's full names should never be used and images of children should never be shared via WhatsApp. All communications must be respectful and professional and all adults should be aware that the content of WhatsApp can be considered as evidence in safeguarding or disciplinary issues.

The Organisation reserves the right to monitor ICT and Email usage.
Any breach of this policy can be considered as a disciplinary matter and dealt with accordingly through the organisation's disciplinary procedure.

Adult use of email

Adults should work within the organisation's policies for safe data management and record keeping. Data on children should only be shared through secure platforms. Once an email is written about an individual, they could have the right to view that data. Only the Head Teacher, School Administrators and Senior Teachers should send information about young people via email to external agencies. If anyone needs information sent, they should ask one of these adults to send it, using the appropriate secure system
Passwords must be kept secure and adults must log out of individual devices, email accounts, BehaviorWatch and the Google Drive when they are away from their desks and machines. Google mail accounts are owned and run by the organisation and are subject to scrutiny and Emails should never be used to share inappropriate, defamatory, illegal or discriminatory material.
Adults are required to manage their email storage responsibly — email inboxes are not a storage facility and should be kept tidy through deletion and the creation of subfolders. Personal data should be managed under the Data Protection Act 1998. Adults must be informed that emails can be used as evidence in a court of law, and once sent exists in multiple locations. Offensive or threatening emails must be reported to the Head Teacher.
It is perfectly acceptable for adults who work at the Lioncare School to access their emails off site and at home as email is often the most effective form of communication in a number of situations. However adults are expected to take all reasonable steps to secure access to their email accounts on any personal equipment. This means email accounts must be password protected, as must the devices used to access them and adults must log out of their accounts when not directly using their accounts. Browser security settings must be optimised and any adult who is unsure how to manage their settings needs to take personal responsibility in updating their skills and knowledge

The Google Drive and behaviour watch can be accessed from home laptops and desktop machines that are password protected as long as all other safe practices are observed (logging out, safe settings etc.) but these sites should not be accessed from personal mobile devices unless there at least two levels of security in place to prevent accidental or malicious usage. Images of children should never be accessed from personal devices, on or off site.

Visitors to the school

All adults visiting the Lioncare School will be advised that if they choose to use their personal portable devices on site that this can only be done within the guidelines set out in this policy. For visitors who cannot complete tasks without the use of devices (Consultants, Trainers, Inspectors etc.) this means they will need time to look at the policy and for a verbal briefing from either the DSL/DDSL or a school administrator before work commences. A card stating the following will be handed to them for the duration of their visit.

Welcome to The Lioncare School
During our signing in process you have identified that while in school you will be working on your personal portable device. This note is to make certain that you are aware that any such usage is covered by our online safety policy. You will be briefed on this by either one of our administration team or the safeguarding lead and her deputies. In summary this means:

- *You are personally responsible for the security of your device at all times; a locked cupboard can be provided if you request.*
- *Your device should never be given to, or accessed by, a child. If you lose your device you must tell someone immediately.*
- *All content accessed by, or viewed by you, during your visit must be related to your professional task*
- *On no occasion, or for any reason, can content related to pornography, child exploitation or political extremism be accessed or viewed while at the Lioncare School. If this is observed or picked up by our filter, we have the right to consider making a referral to safeguarding agencies, including the police.*

Thank you for your attention to this note.

Management Information Systems

The Lioncare School use two Management Information Systems:
Behaviour Watch
This system is used to report on, share and track trends in behaviour for individuals and for groups in school. It also is used to track progress data for individuals and groups and as a live source of current information. It is a web-based system and is password protected. It can be appropriate for adults to access Behaviour Watch when off site and the following should be kept in mind:

- Behaviour Watch allows system administrators to audit who has logged in and any edits they have made to documents within the system, the time of these edits is recorded.
- Adults are only given the level of access deemed necessary for their role
- Adults are responsible for any activity that happens under their log in, this includes unauthorised access by children.

- Adults may only access behaviour Watch on devices that are password protected and adults must log out of their accounts when not directly using their accounts.
- The auto log-in function should never be in operation.
- Browser security settings must be optimised and any adult who is unsure how to manage their settings needs to take personal responsibility in updating their skills and knowledge and personal machines should never be set to "remember password"
- No document should be downloaded or printed onto or from a machine not owned by the Lioncare Group
- If adults involved in an activity or event assess that they are likely to need access to Behaviour Watch in order to keep accurate records the activity plan should indicate a school owned device is taken by adults.
- An adult may wish a child to sit alongside them while key work or reflective forms are filled in. The adult must lead the task and have control of the keyboard and mouse and only the form screen should be available. Non compliance should lead to the end of the activity.

The Google Drive

The Google Drive is the main storage system for information for the Lioncare Group and the site of many working documents. There are many situations in which it is appropriate for adults to access the Google Drive off site for pre-agreed and specific work tasks. The following should be kept in mind at all times:

- The Google drive allows users to audit who has logged in and any edits they have made to documents within the system, these edits are time stamped.
- Adults are only given the level of access deemed necessary for their role and the Head Teacher and the executive team reserves the right to restrict access as necessary for the safe, effective and compliant functioning of the school.
- Adults are responsible for any activity that happens under their log in
- Adults may only access The Google Drive on devices that are password protected and adults must log out of their accounts when not directly using their accounts.
- Browser security settings and the sharing permission settings for folders must be optimised and any adult who is unsure how to manage their settings needs to take personal responsibility in updating their skills and knowledge and personal machines should never be set to "remember password"
- No document containing the personal information of children or adults should be downloaded or printed onto or from a machine not owned by the Lioncare Group
- The Head Teacher, School Online Safety coordinator and other senior managers will monitor usage of the Google Drive by adults. This will be done to help promote a positive approach to upholding boundaries between work life and personal life but will also ensure that access is only related to pre-agreed and specific work tasks
- All tasks that related to the planning of teaching, learning and school activities, the checking of policies and procedures, the formulation of risk assessments, the updating of message logs, accessing training and academic materials and the monitoring of school improvement plans or other tasks that do not require access to any personal information and/or records are deemed as pre-agreed and specific work tasks.

It is recognised that there may be rare occasions or situations where an employee is legitimately required to access other areas of the Google Drive where personal information is stored using their Personal Computer at home or Personal Laptop Computer or personal portable device, for example if they are needing to work from home for a period of time due to a reasonable adjustment to their working conditions that prevents them from attending their place of work, or if they are undertaking a specific piece of work for and on behalf of the organisation away from the work-place and do not have access to a Laptop owned by and/or monitored by and/or sanctioned by The Lioncare Group or some other similar situation. In such situations the employee is required to and must first seek and gain explicit written permission to do so from the Head Teacher and to provide written agreement and confirmation that the necessary special precautions have been implemented to ensure such use is and remains safe and secure and where such authorised employees have provided an agreement that they will ensure any such use is carried out in such a way that the confidentiality and security of information concerning colleagues and the children in our care is guaranteed at all times.

Training, Development and Professional Support

A number of structures are in place to ensure adults understand their responsibilities:

- During the first week of induction all staff are required to read this policy, the guide to Safer Working Practice and the Safeguarding and Child Protection Policy ready for professional discussion in 1:1 supervision
- All of these issues are regularly brought to supervision and daily debrief for discussion and, where necessary, challenged.
- All adults are expected to undertake Level 2 E-safety awareness training in the first year of employment
- All adults are expected to re-sign the classroom safety guidelines alongside Children and Young People at the start of each term.
- All adults are expected to participate in Safer Internet Day
- In April of each year there is a whole team safeguarding training which includes aspects of online safety
- In September of each year time in team meetings is given to whole team updating of revised policies and how content will be embedded in practice

The DSL and DDSL attend training via the LSCP network and through the Lioncare School's NASS Membership

System Security

The Head Teacher, in partnership with the school administrators and the organisation's ICT consultant, ensures that the school ICT system is reviewed regularly with regards to security.

- Users must lock or log out from computers when leaving the computer for any period of time.
- Users must use only their own personal user account, with the exception of younger young people who will use the Caterpillar class account and logged in by an adult, and home adults in school who will use the Handovers account for completing handover.
- Adults and older young people will be expected to create their own secure passwords.
- User account passwords will be changed if they become known.
- Anti-virus protection is installed on all equipment and will be updated regularly. Daily anti-virus scans will be scheduled on all equipment.
- The security of individual staff and pupil accounts will be reviewed regularly by the online safety coordinator
- Computers (including mobile devices) may not be connected to the school network either physically or wirelessly without specific permission.

- There will be separate wireless networks for adults and young people, and the passwords can be changed if they are accessed without permission.
- The young people's Wi-Fi password is not given to young people, instead an adult will enter it into wireless devices for them.
- Personal data sent over the Internet will be encrypted or otherwise secured where possible.
- Portable media may not be used without specific permission followed by a virus check. It is unlikely that permission will be given for portable USB storage to be used.
- Users will only download images and documents, and only open files from websites they recognise and trust.
- Unapproved system utilities and executable files will not be allowed in children and young people's work areas or attached to emails.
- Software will not be installed/removed from computers without specific permission, and school mobile devices will be configured with 'parental controls' to prevent downloading of apps without specific permission.
- Files will not be moved or removed from a shared folder without specific permission.
- Adults and young people's files and folders will be kept in separate work areas, with users only able to access their own files and relevant shared folders.
- The ICT coordinator / school administrator will review system capacity regularly.
- Backups of the entire system will be made regularly on a minimum of three encrypted removable media, with one kept off-site and all rotated weekly

Protection of Personal Data (please refer to the organisation's record management policies for full detail)

Personal data will be recorded, stored, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation 2018.
Our young people have complex backgrounds and we hold sensitive information in school to help us develop appropriate child centered behaviour management plans. We treat this data and any other personal data related to children, young people and adults with the utmost care. All online systems are password protected and nothing is shared without sound reasons and safe systems in place. Adult personnel files are not saved onto the google drives but to the Shared drive at our head office, which is only accessible by the executive Team and their administrators.
In line with the Data Protection Act 1998, and the General Data Protection Regulation 2018 and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data longer than is necessary

- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the police. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect. Where there is any ambiguity the Head Teacher reserves the right to refuse to share data until the situation is clarified. Where possible any data shared with local authorities is done so via a secure email system and only key senior staff have permission to email out personal data on individuals or cohorts of learners.
Breaches of Data will be reported to the ICO within 72 hours.
The Lioncare School does not utilise or store biometric data.

Published Content

The Lioncare School has a duty under the law (Independent School Regulations 2014, Paragraph 6) to make certain information available to the public. It chooses to do this via its website http://lioncare.co.uk/therapeutic-education/lioncare-school/
The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and data protection policies. Adult photographs are in our prospectus but no contact details are given. All numbers and email addresses are for administrative teams apart from that of the Head Teacher. Contact details for the DSL and DDSL are in the Safeguarding and Child Protection Policy which is published on the website. In all such cases only work email addresses and the office phone numbers are given.

No other details of adults or children are ever published on the website. No images that can identify individual children are used in any material for publication or marketing purposes and the names of individual children are not publicly shared on any occasion.
The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. As of August 2020, only the Executive Director of the Lioncare Group had authority and access to upload material to the website.

Sources of Support and information

Taken from Keeping Children Safe in Education 2021 Annex D:

Online Safety Information and support There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:
Advice for governing bodies/proprietors and senior leaders :

Childnet provide guidance for schools on cyberbullying • Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation • London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements • NSPCC provides advice on all aspects of a school or college's online safety arrangements • Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective • Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones • South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements • Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq • UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring • Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk. • Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's 151 personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Remote education, virtual lessons and live streaming :
Case studies on remote education practice are available for schools to learn from each other • Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely • London Grid for Learning guidance, including platform specific advice • National cyber security centre guidance on choosing, configuring and deploying video conferencing • National cyber security centre guidance on how to set up and use video conferencing • UK Safer Internet Centre guidance on safe remote learning Support for children • Childline for free and confidential advice • UK Safer Internet Centre to report and remove harmful online content • CEOP for advice on making a report about online abuse

Parental support : Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support • Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents • Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying • Government advice about security and privacy settings, blocking unsuitable content, and parental controls • Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world 152 • Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation • London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online • Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online) • National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online • Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps

and games • Parentzone provides help for parents and carers on how to keep their children safe online • Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations • UK Safer Internet Centre
Acknowledgements Some aspects of this policy are based on the Optimus Education Model Policy http://my.optimus-education.com/school-model-policy-templates-meet-your-legal-requirements