ICT and ONLINE SAFETY POLICY

Reviewed and updated 10.09.2025

ICT

Introduction

Information and Communications Technology prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. We recognise that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and using critical thinking.

Our vision is for all teachers and learners in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which enable them to use appropriate ICT resources effectively as powerful tools for teaching & learning.

Following the law

In addition to prohibitions against violating the fundamental values of the French national curriculum – in particular the principles of neutrality (religious, political and commercial) - the following are forbidden and subject to sanctions:

- Any violation to a person's right to privacy;
- Defamation and verbal abuse;
- Cyber-bullying in all forms
- Identity theft
- Inciting minors to commit illegal or dangerous acts, encouraging the corruption or depravity of minors, the use of any picture of a minor for pornographic ends, the distribution of messages with violent, graphic or pornographic subtext likely to be seen by minors;
- Encouraging the consumption of illicit substances;
- Inciting the perpetration of criminal acts and inciting suicide, inciting discrimination, hate (particularly racial hate) or violence;
- Justifying or eulogizing any crime, in particular murder, rape, war crimes and crimes against humanity; denying crimes against humanity;
- Counterfeiting brands;
- Reproducing, representing or disseminating intellectual property (for example: musical extracts, photography, literary passages, etc.) or benefitting from related rights (for example during the performance of a composer's work, audio or visual recordings, programs belonging to an audio- visual communications company**)** in violation of the author's rights, the owners of related rights and/or the holders of the rights to intellectual property;
- Copying commercial software for any use whatsoever, with the exception of one copy safeguarded in accordance with the terms set out by the holders of intellectual property.

Aims

- To enable children to become autonomous, independent users of ICT, gaining confidence and enjoyment from their ICT activities
- To develop a whole school approach to ICT ensuring continuity and progression in all strands of the ICT National Curriculum
- To use ICT as a tool to support teaching, learning and management across the curriculum
- To provide children with opportunities to develop their ICT capabilities in all areas specified by the Curriculum.
- To ensure ICT is used, when appropriate, to improve access to learning for pupils with a diverse range of individual needs, including those with SEN and disabilities
- To maximise the use of ICT in developing and maintaining links between other schools, the local community including parents and other agencies.

Objectives

In order to fulfil the above aims it is necessary for us to ensure:

- a continuity of experience throughout the school both within and among year groups
- the systematic progression through key stages 1 & 2
- that all children have access to a range of ICT resources
- that ICT experiences are focussed to enhance learning
- that cross curricular links are exploited where appropriate
- that children's experiences are monitored and evaluated
- that resources are used to their full extent
- that resources and equipment are kept up to date as much as possible
- that staff skills and knowledge are kept up to date

Equal Opportunities

The National Curriculum states that, "All pupils, regardless of race, class or gender, should have the opportunity to develop ICT capability."

It is our policy to ensure this by:

- ensuring all children follow the scheme of work for ICT
- keeping a record of children's ICT use to ensure equal access and fairness of distribution of ICT resources
- providing curriculum materials and software which are in no way class, gender or racially prejudiced or biased
- monitoring the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged

Online Safety

The 4Cs

Being online can be a great source of fun, entertainment, communication and education. Some people's online behaviour places others at risk. The number of issues covered under online safety is large and constantly growing. They are categorised into these four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users, for example 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: online behaviour that increases the likelihood of, or causes, harm, for example making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying).

Commerce: risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, could sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. This is why we have decided that should parents request that any children in CM1 or CM2 bring a mobile phone to school, it must be switched off, handed in to the teacher and stored away until the end of the school day. Please also consult the School's **Mobile Phone Policy**.

Roles and Responsibilities

School management will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Ensuring staff receive regular, up-to-date and appropriate Safeguarding training including online safety.
- Working with the DSL and IT coordinator to conduct reviews of this policy as appropriate.

The DSL will be responsible for:

- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff, e.g. the SENCO and IT Coordinator, on online safety matters.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities.
- Reinforcing the procedure for reporting online safety incidents and inappropriate internet use, both by pupils (to a trusted adult – teacher;DSL or DDSL) and staff (directly to the DSL or the DDSL and onto the MyConcern platform), and ensuring all members of the school community understand this procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends.

The IT Coordinator will be responsible for:

- Providing technical support in the development and implementation of the School's online safety policies and procedures.
- Implementing appropriate security measures as directed by the school management.
- Ensuring that the filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network and how often pupils access the network.
- Ensuring that anti-virus software is kept up to date and managed.
- Ensuring that firewalls are switched on at all times.
- Managing staff's Microsoft two-step verification for enhanced security

All Staff Members will be responsible for:

- Taking responsibility for the security of the ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Using the approved class email accounts and the ClassDojo app to communicate with parents and the school community at school and when doing school-related work outside of school hours.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

- Seeking help from school staff, in line with the procedures within this policy, if they are concerned about something they or a peer have experienced online.

Internet Access and Supervision

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

Handling Online Safety Concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy. Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future.

Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported. The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the

DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information.

If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the DSL (or DDSL), who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the LADO (Local Authority Designated Officer).

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT coordinator, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy. Where there is a concern that illegal activity has taken place, the DSL contacts the police. The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy. All online safety incidents and the school's response are recorded and managed by the DSL.

Internet Safety

The user may only use computers/tablets/ interactive whiteboards and the internet under the supervision of an adult.
Internet access is planned to enrich and extend learning activities.
The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies.

Keeping Children Safe in Education obliges schools to "ensure appropriate filtering and 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."
In line with this, although the school offers a safe online environment through a secure BT hub connection and filtered internet access, we recognise the importance of teaching our children about online safety and their responsibilities when using communication technology.

Protecting pupils

It falls to the school and its educational team to regulate any activity linked to the services it provides - particularly through constant monitoring of pupils' activities so as to be in a position to intervene rapidly should any problems arise.
It is also the school and its educational team's responsibility to ensure, on a case by case basis, that the activities which it organizes are undertaken in a secure environment. Given their involvement and proximity

to educational activities, it is up to teachers to ensure that the appropriate protection mechanisms are in place so as to safeguard children from illicit content (and any content which glorifies crime, theft, hatred, debauchery or any materials regarding crime/delinquency likely to negatively impact upon the children, as well as material which may inspire or entrench racial prejudice).

The Classroom Teacher

Even though whole school co-ordination and support is essential to the development of ICT capability, it remains the responsibility of each teacher to plan and teach appropriate ICT activities and assist the specialist teacher in the monitoring and recording of pupil progress in ICT. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Pupils will be supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Physical Safety

We will operate all ICT equipment in compliance with Health & Safety requirements. In order to reduce the risk of musculoskeletal issues and eye strain, children will be made aware of the correct way to sit when using iPads and laptops and the need to take regular breaks. We will ensure device use is in well-lit areas, where screens are visible to allow for circulating staff supervision.

Effective and efficient deployment of ICT resources

ICT resources, such as iPads and laptops are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment.
To enable regular and whole class teaching of ICT the school has installed an interactive smart board in most classes.
To support the cross curricular nature of ICT at least one computer is also located in each class with 15 iPads also available for classroom usage. These are also used for additional tasks which require the use of ICT.

Precaution measures to ensure safe internet access for our children at all times:

• All devices are connected to the internet through a secure Wi-Fi network and using a search engine with filter settings engaged. Children are taught to access this as appropriate.
• All class interactive boards have an integrated safe mode for search engines.
• Children use Google search with safe mode on iPads (children cannot chat, access social media sites, or access the App store).
• Staff will select sites and apps which will support the learning outcomes planned for children.
• Internet access will be planned to enrich and extend learning activities.
• Children are directly supervised when using the internet but are expected to share immediately with the teacher any material that they think is inappropriate.
• Children will be given clear guidance for internet use, and only ever be allowed to access approved educational sites selected by staff.
• The children will never be given access to unsupervised open chat rooms.

The school has the view of not over filtering websites so that children have a safe environment to learn how to make the right choices if they see something they are not happy with.

The school recognises its responsibility to educate our children to protect themselves in and outside of school.

To this end:

• Children will be made aware of issues surrounding uncertainty of online identities and revealing personal data.
• When online safety trends occur, the school will make a decision as to whether to share safety concerns with pupils to make them aware or may choose not to inform pupils so that we are exposing it issue to them unnecessarily.
• Online safety will be covered in assemblies and in lessons
•The school carries out appropriate monitoring and filtering of internet use.
•Should an issue arise (children mentioning using apps such as Instagram or WhatsApp outside of school, that they are too young for, for example) which possibly highlights online safety concerns then teachers will either contact the whole class or individual parents.

The following information is taken from the NSPCC website and or DfE's Keeping Children Safe in Education.

Cyberbullying

Cyberbullying is a growing problem and includes:
• sending threatening or disturbing text messages.
• Discriminatory bullying online, i.e. homophobia, racism, misogyny/misandry.
• making silent, hoax or abusive calls.
• creating and sharing embarrassing images or videos.
• trolling; the sending of menacing or upsetting messages on social networks, chat rooms or online games.
• Unpleasant or defamatory information posted to blogs, personal websites and social networking sites.
Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible.
• encouraging young people to self-harm.
• hijacking or stealing online identities to embarrass a young person or cause trouble using their name.
The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying policy.

Child-on-Child Sexual Abuse and Harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:
• Threatening, facilitating or encouraging sexual violence
• Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
• Sexualised online bullying, e.g. sexual jokes or taunts

- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Behaviour Policy and the Safeguarding and Child Protection Policy.

Sharing of nudes and semi-nudes (This used to be referred to as Sexting)

This is just as relevant in the upper primary years as with secondary school years. Children are having earlier experiences with using social media sites and new Apps (sometimes with parental permission, sometimes secretly) even though the age restrictions on these are quite clear.

All schools should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children.

NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. Please also refer to the schools Safeguarding and Child Protection Policy for how to respond to an incident of Sharing nudes and semi-nudes, as it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The school DSL will in turn use the full guidance document, *Sharing nudes and semi-nudes – advice for educational settings* to decide next steps and whether other agencies need to be involved.

Consider the following 5 points for immediate referral at initial review:

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

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.
The document referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. DfE guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' (such as bra-strap flicking and the careless use of language) are treated seriously and not allowed to perpetuate.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.
Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.
Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse.
The DSL will ensure that safeguarding training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet.

In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence.

While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.

Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Preventing Radicalisation Policy.
Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.
Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay.

Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively.

The School will ensure, via Safeguarding training sessions, that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.

Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.
The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.
Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely. Prior to deciding

how to respond to a harmful online challenge or hoax, the DSL will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Safeguarding and Child Protection policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate. The DSL, together with school management, will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.
The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.
The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Social Media

Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, L'école Bilingue will request that the post be deleted and will expect this to be actioned promptly.
Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.
Parents also need to be aware that 'sharenting' can be harmful to children's self-esteem. This is where parents put images and pictures of children online which are later found to embarrass them as they get older.

Staff, pupils' and parents' social media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it.
However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years.

The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise.

Online safety lessons/assemblies will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse.

Email to admin@lecolebilingue.uk is the official electronic communication channel between parents and the school. Electronic communication between staff and parents, aside from class emails, will be carried out using school accounts for educational purposed only, through the following platform: ClassDojo

Staff must not follow public student accounts. Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online.

They should never discuss the school on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute. (Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher, and should be declared upon entry of the pupil or staff member to the school).

Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL. All members of the school community are reminded that particularly in the context of social media, it is important to comply that permission is sought before uploading photographs, videos or any other information about other people.

Recording Online-Safety Incidents

• Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
• Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships and Sex Education (RSE) and Health education curriculum.
This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives.
This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
• General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of caution by talking to the designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem

The use of digital images and video

To comply with the General Data Protection Regulation (which supersedes the 1998 Data Protection Act), we need parents' permission before we can photograph or make recordings their daughter(s) / son(s).

The School rules for any external use of digital images are:
• Staff are not allowed to take photographs or videos on their personal equipment.
Examples of how digital photography and video may be used at school include:
• Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity, e.g. taking photos or a video of progress made in a lesson.
•Your child's image being used for presentation purposes around the school, e.g. in class or wider school wall displays
• Your child's image being used in order to share its good practice and celebrate its achievements, which is shown to other parents, e.g. on ClassDojo or on our school website. On rare occasions, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event. Permission will always be sought in these circumstances.
Note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if they won a national competition and wanted to be named in local or government literature.

Monitoring and Review

The School recognises that the online world is constantly changing; therefore the DSL, DDSL, school management and the IT Coordinator will conduct regular reviews of this policy.

Legal Framework:

- **“Keeping children safe in education”, DfE, 2025**
- **Guidance: Sharing nudes and semi-nudes: how to respond to an incident (overview) (updated 11th March 2024**
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) ‘Filtering and monitoring standards for schools and colleges’

Linked Policies:

Safeguarding and Child Protection Policy
Staff Behaviour Policy
Mobile Phone Policy
Whistleblowing Policy