

ICT /Online Safety Policy

Reviewed and updated 04 October 2024

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 Information and Communications Technology is an important tool in both the society we live in and in the process of teaching and learning. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources.

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 also 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 2000 orders.
- 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

Teaching & Learning

Teacher's planning is differentiated to meet the range of needs in any class including those children who may need extra support, those who are in line with average expectations and those working above average expectations for children of their age.

A wide range of styles are employed to ensure all children are sufficiently challenged:

- Children may be required to work individually, in pairs or in small groups according to the nature or activity of the task.
- Different pace of working
- Different groupings of children - groupings may be based on ability either same ability or mixed ability.
- Different levels of input and support
- Different outcomes expected

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

Internet Access and Supervision

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 filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”

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, especially minors

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, and to notice and put an end to any behaviour likely to turn violent.

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.

Health & Safety

We will operate all ICT equipment in compliance with Health & Safety requirements. Children will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers.

Effective and efficient deployment of ICT resources

ICT resources 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.

Online Safety

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: 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, and

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, 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.

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
- Staff will discuss suitable time to spend online as to promote positive mental health.

- 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. These issues will be discussed with children in classes at an age-appropriate level.

Cyberbullying

Cyberbullying is a growing problem and includes:

- sending threatening or disturbing text messages.
- homophobia, racism or sexism.
- 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.
- excluding children from online games, activities or friendship groups.
- setting up hate sites or groups about a particular child.
- encouraging young people to self-harm.
- voting for someone in an abusive poll.
- hijacking or stealing online identities to embarrass a young person or cause trouble using their name.

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 (regardless of phase) 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 Child Protection and Safeguarding 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 DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise. 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. The 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' are treated seriously and not allowed to perpetuate.

The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

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 (note that WhatsApp is 16+).

Online safety lessons 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.

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 (if by a child) or to the Headteacher (if by a staff member).

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 education, 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

Reference:

“**Keeping children safe in education**”, DFE, 2024

Guidance: Sharing nudes and semi-nudes: how to respond to an incident (overview) (updated 11th March 2024

<https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-how-to-respond-to-an-incident-overview>

Linked Policies:

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