First Coding Ltd - Online Safety Policy

Scope of the Policy

This policy applies to all members of First Coding Ltd*'s* community (including staff, young people, volunteers, parents/carers, visitors, and community users) who have access to and are users of our digital technology systems, both in and outside of First Coding's teaching venues..

First Coding Ltd will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place outside of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within First Coding Ltd:

The Online Safety Lead is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Online Safety Lead receiving regular information about online safety incidents and monitoring reports.

Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT/relevant body
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,

Staff and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current First Coding Ltd online safety policy and practices
- they have read, understood, and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to *Online Safety for* investigation/action/sanction
- all digital communications with young people/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the activities
- young people/participants understand and follow the Online Safety Policy and acceptable use policies
- young people/participants have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in workshops and other activities (where allowed) and implement current policies regarding these devices

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

(N.B. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. Some organisations may choose to combine the roles of Designated Safeguarding Lead and Online Safety Lead).

Young People/Participants

- are responsible for using the digital technology systems in accordance with the acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online bullying.

- should understand the importance of adopting good online safety practices when using digital technologies out of First Coding Ltd and realise that First Coding Ltd*'s* online safety policy covers their actions out of First Coding Ltd, if related to their membership of First Coding Ltd

Parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. First Coding Ltd will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media, and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support First Coding Ltd in promoting good online safety practices and to follow guidelines on the appropriate use of

- digital and video images taken at events
- their children's personal devices in First Coding Ltd(where this is allowed)

Policy Statements

Education – Young People/Participants

Whilst regulation and technical solutions are very important, their use must be balanced by educating *young people* to take a responsible approach. The education of *young people* in online safety/digital literacy is therefore an essential part of First Coding''s online safety provision. Children and young people need the help and support of staff to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas and staff should reinforce online safety messages across the programmes. Online Safety learning should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Key online safety messages should be reinforced as part of a planned
- Young People/Participants should be taught in all sessions to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Young People/Participants should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Young People/Participants should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Young People/Participants should be helped to understand the need for the student/pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside First Coding Ltd.
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices
- In lessons where internet use is pre-planned, it is best practice that Young People/Participants should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where Young People/Participants are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand First Coding Ltd online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Technical – infrastructure/equipment, filtering and monitoring

If First Coding Ltd has a managed ICT service provided by an outside contractor, it is the responsibility of First Coding Ltd to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of First Coding Ltd, as suggested below. It is also important that the managed service provider is fully aware of First Coding Ltd online safety policy/acceptable use

agreements. First Coding Ltd should also check their Local Authority/MAT /other relevant body policies on these technical issues.

First Coding Ltd will be responsible for ensuring that First Coding Ltd infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: (schools/academies will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational, and administrative staff before these statements are agreed and added to the policy:)

A more detailed Technical Security Template Policy can be found in the appendix.

- First Coding Ltd's technical systems will be managed in ways that ensure that First Coding Ltd meets recommended technical requirements (these may be outlined in Local Authority/MAT/other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of First Coding Ltd's technical systems
- Servers, wireless systems, and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to First Coding Ltd technical systems and devices.
- First Coding Ltd is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users via the ISP's Parental Controls. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on "appropriate filtering").
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.

Responding to incidents of misuse

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

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer it to the appropriate First Coding person who is responsible for online safety incidents and report immediately to the police.

Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off-site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

- If the content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

First Coding Ltd actions & sanctions

It is more likely that First Coding Ltd will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

First Coding Ltd is committed to reviewing our policy and good practice annually.

This policy was last reviewed on : 05/08/24

Signed: J Whitworth

Date: 05/08/24