The Croft Preparatory School

Online Safety Policy

Whole School Policy, including Early Years Foundation Stage

Policy reviewed (LMi)	17 October 2023
Peer Review completed	14 November 2023
Approved SLT	21 November 2023
Next Review Date	October 2024

The legal responsibility for ensuring that the Croft Preparatory School adheres to all relevant statutory regulations, as issued by the DfE, lies with the Proprietors. At their discretion, the Proprietors may delegate the monitoring of the efficacy with which the school discharges its statutory duties to the Board of Directors and the Governing Committee.

Notwithstanding the above delegation, the Proprietors retain ultimate responsibility for how the statutory functions are executed.

Table of Contents

Section A - Policy and Leadership

The key individuals responsible for implementation of the School's Online Safety strategy are as follows:

A.1 Responsibilities:

Online Safety Coordinator

The Online Safety Coordinator is responsible to the Headmaster and Governors for the day-to-day issues relating to the IT infrastructure and online safety. **The role of Online Safety Coordinator is currently held by the Deputy Headmaster, who is also the School's Designated Safeguarding Lead.**

The Online Safety Coordinator ensures:

- the school's IT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the online safety technical requirements outlined in Section B of this policy
- users may only access the school's networks through properly enforced password protection
- shortcomings in the infrastructure are reported to the Headmaster so that appropriate action may be taken
- chairs the Online Safety Committee which meets termly and comprises of the Head of Technology & ICT and nominated children from the school
- 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
- provides training and advice for staff
- liaises with appropriate external bodies
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- regularly reviews the output from monitoring software and initiates appropriate action where necessary
- considers unblocking requests and instructs IT contractors to act as appropriate

- attends relevant meetings of the Governing Committee to discuss current issues and review incident logs

- reports regularly to the SLT Meeting and SMT on online safety matters

- receives appropriate training and support to fulfil the role effectively

The Board of Directors and the Governing Committee

The Board of Directors and the Governing Committee are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out through both bodies receiving regular information about online safety incidents and monitoring reports provided by the Online Safety Coordinator.

Headmaster

The Headmaster is responsible for ensuring the safety (including online safety) of all members of the school community.

Day to day responsibility for online safety is delegated to the Online Safety Coordinator.

The Headmaster is responsible for ensuring the correct procedures are followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in section A.8)

Staff

Teaching and support staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices

- they have read and understood the following documents:

    - Staff code of conduct
    - Data Protection and Retention Policy
    - Information Security and Data Breach Policy

- they report any suspected misuse or problem to the Online Safety Coordinator

- digital communications with pupils and parents/carers are always on a professional level and only carried out using official school systems (see A.13)

- online safety issues are embedded in the curriculum and other school activities (see section C)

The Online Safety Committee – Scope and Function

The Online Safety Committee meets termly to:

- Review and monitor the Online Safety Policy

- Consider any issues relating to school filtering (see section B.2.1)

- Discuss any online safety issues that have arisen and how they should be dealt with

Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Warwickshire Safeguarding Children Board.

A.2 Policy development, monitoring and review

This Online Safety Policy is reviewed annually by

- The Online Safety Coordinator
- Head of Technology
- The online safety committee

Communication with the whole school community takes place through the following:

- Staff meetings and training days
- Governors' meetings
- Parents' Evenings
- School website and other communications

A.3 Policy Scope

This policy applies to **all members of the school community** (including senior leaders, teaching staff, support staff, pupils, volunteers, Governors, parents/carers, visitors, community users and contractors) who have access to and are users of school ICT systems, **both in and out of school**.

The Education and Inspections Act 2006 empowers the Headmaster, on behalf of the Proprietors, to such extent as is reasonable, to regulate the behaviour of pupils when

they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying or other online safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as the Good Behaviour and Anti-bullying Policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

A.4 Acceptable Use Agreements

All members of the school community are responsible for using the school computer systems in accordance with the staff code of conduct and or pupil acceptable use policy.

The staff code of conduct is provided to all staff, including temporary and cover staff, on commencement of their employment at the school.

Acceptable use agreements are provided for pupils arriving in Year 1 and upwards. These agreements are signed by the children and their parents.

The agreements are sent out in the Michaelmas Term by administration staff and are returned to the Main School Office to be stored in pupil files. Computing teachers go through the detail of the agreements with pupils during lessons, to ensure that children understand the requirements (this is communicated to them through their Online Safety Lessons).

A.5 Self-Evaluation

Evaluation of online safety is an ongoing process and links to other self-evaluation tools used in school, in particular to pre-inspection ISI evaluations along the lines of the Self-Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parents, teachers and others) are taken into account as a part of this process.

A.6 Whole School approach and links to other policies

The Online Safety Policy has strong links to other school policies as below:

- **Safeguarding and Child Protection Policy** - Safeguarding children electronically is an important aspect of online safety. The Online Safety Policy forms a part of the school's overall safeguarding policy

- **Low-Level Concern Policy**

- **Computing Policy** - How computing is taught, managed and supported in school

- **Internet and Email Acceptable Use Policy All Pupils**

- **Anti-bullying Policy** – How the school strives to eliminate bullying and cyberbullying

- **PSHE** - Online safety has links to staying safe and healthy/unhealthy relationships

- **Relationships and Sex Education Policy –** providing a framework in which sensitive discussions can take place

- **Information Security and Data Breach Policy**

- **Staff code of conduct**

- **Data Protection and Retention Policy** - How the school protects and retains information

- **Good Behaviour -** Positive strategies for encouraging online safety and sanctions for disregarding it

- **Use of Photographic Images Policy -** How photographic material is used in school and on other platforms

A.7 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (**in or out of school**).

Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (The Protection of Children Act 1978)**

- **grooming, incitement, arrangement or facilitation of sexual acts against children (Sexual Offences Act 2003)**

- **possession of extreme pornographic images (Criminal Justice and Immigration Act 2008)**

- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (Public Order Act 1986)**

- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable on computer devices equipment or infrastructure provided by the school:

- Using school systems to run a private business
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling and non-educational gaming
- Online shopping/commerce, other than where specifically authorised to do so for school purchasing purposes
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school or necessary for the individual's role)

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is probable that the school 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, and that members of the school community are

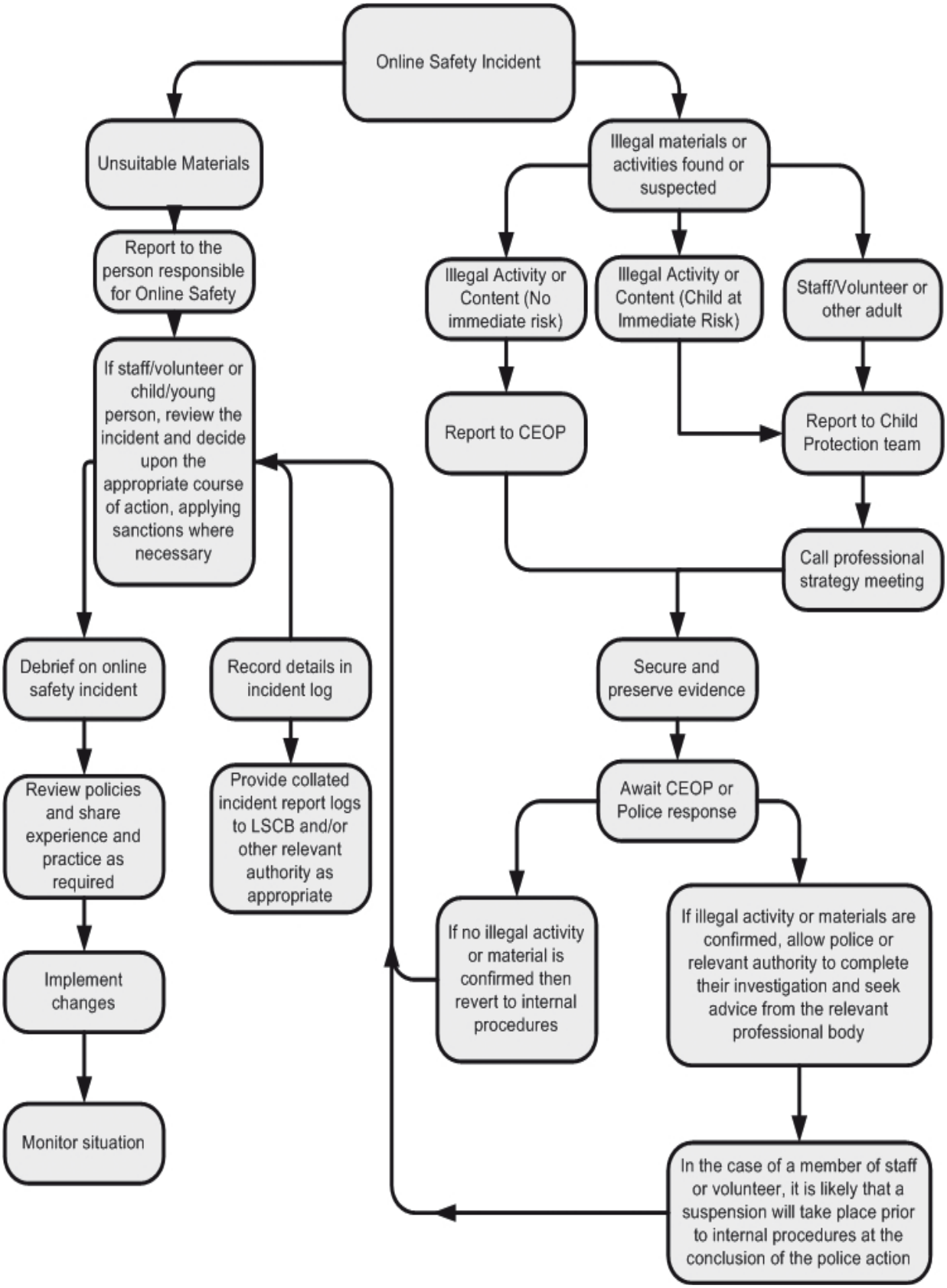
aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Any instance of a child or parent posting defamatory or personal comments about any member of staff on any social media website, regular website or in any email brought to the school's attention, may result in the suspension of the offending child while the matter is investigated. Such conduct could lead to expulsion of the child if the incident is deemed to be malicious and harmful to either an individual staff member or the school as a whole.

A.8 Reporting of online safety breaches

It is hoped that all members of the school community will be responsible users of all form of digital devices, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse. Listed below in the flow chart are the responses that will be made to any apparent or actual incidents of misuse.

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.7 of this policy.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

A.9 Use of handheld technology (personal phones and handheld devices)

We recognise that the area of mobile technology is rapidly advancing and it is our School's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are responsible for their own behaviour regarding the use of mobile phones and should avoid putting themselves into compromising situations, which could be misinterpreted and lead to potential allegations.
- Staff members are permitted to use mobile phones within the School, and the classroom, as a technological aid only – for example, as a watch, for personal memory cards, calendar or to access work-related email. Photographs or videos containing pupils should not be taken on personal mobile phones (except where the staff member is the child's parent).
- Mobile phones should not be used in toilets, changing rooms, showers or nappy changing areas within the School. In Early Years, mobile phones should be locked in staff lockers not held on the employee unless on the express permission of the Early Years Manager.
- Personal mobile phones should never be used for contacting parents, except in an emergency such as when working from home during Parent Evenings and the school machine Teams software fails, or on a school trip when the school phone fails.
- Individuals who bring mobile phones into the School should ensure that they do not hold inappropriate or illegal content.
- Staff members are also asked to be alert to the possibility of mobile phone misuse by any parent, visitor, work experience student, contractor or volunteer on the premises and should report any concerns immediately to the DSL for Safeguarding or his deputy.
- Pupils are not currently permitted to bring their personal handheld devices into school unless specifically agreed in advance with parents and teachers.

A.10 Use of communication technologies

Email

Access to email is provided for all employees and all pupils using their personal login details.

These school email services are monitored.

- Users need to be aware that email communications may be monitored.
- Pupils normally use only a class email account to communicate with people outside school and with the permission/guidance of their class teacher.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of, and good practices associated with, the use of email (see section C of this policy)
- Users must immediately report, to their class teacher/Online Safety Coordinator/Line Manager, the receipt of any email that makes them feel

uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Social networking (including chat, Twitter, instant messaging, blogging etc)

The use of non-work-related social media accounts is prohibited for staff or pupils during the working day.

A.11 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images (see section C). In particular, they should recognise the risks attached to publishing their own images on the internet, eg on social networking sites

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images of children should only be captured using school equipment; **the personal equipment of staff should not be used for such purposes. Photographic and video images should be stored on the shared drive only.**

- The Photographic Images Consent Form is completed by all parents/carers to inform the school whether photographs of their children may be published, and where

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute

- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.12) for guidance on publication of photographs.

A.12 Use of web-based publication tools

Website (and other public facing communications)

Our school uses the public facing website www.croftschool.co.uk for sharing information with the community beyond our school. This includes, from time to time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only school email addresses should be used to identify members of staff (never pupils)

- Only a pupil's first name and initial are used on the website, and only then when necessary

- Detailed calendars are not published on the school website

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - ✓ images that can easily be re-edited are not posted in public areas
    - ✓ Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or in any other media

A.13 Professional standards for staff communication

In all aspects of their work teachers abide by Staff Code of Conduct.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems

- Personal email addresses, social media, text messaging or public chat/social networking technology must not be used for these communications

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

Teachers frequently discuss issues relating to password security and how it relates to staying safe in and out of school. All staff are to abide by the School's Password Policy as outlined in the Information Security and Data Breach Policy.

B.2 Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities
Overall responsibility for the management of the school's filtering policy is held by the Online Safety Coordinator (with ultimate responsibility resting with the Headmaster and Board of Directors).

All users have a responsibility to report immediately to class teachers/Online Safety Coordinator any infringements of the school's filtering policy of which they become aware, or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education/training/awareness
Pupils are made aware of the importance of filtering systems through the school's online safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- briefing in staff meetings, training days, memos etc (timely and ongoing).

Parents will be informed of the school's filtering policy through the Pupil Acceptable Use Agreement.

Changes to the filtering system
Where a member of staff requires access to a website for use at school that is blocked, a request should be submitted to the Online Safety Coordinator who will then consider the criteria below before deciding whether or not to proceed by contacting the IT contractor.

Unblocking requests will always be subject to the following criteria:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

The Online Safety Coordinator will be responsible for authorising all requests and instructing external technicians to sanction the unblocking or otherwise.

Monitoring
No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated above. Monitoring takes place as follows:

- The Online Safety Coordinator reviews the Impero console captures on a regular basis (no less than weekly).

- False positives are identified and deleted

- If a word or phrase is being picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians), the word can be allowed for the period of the topic being taught

- The school will monitor pupils use of the internet in accordance with 'The Prevent Duty Guidance' relating to the Counter-Terrorism and Security Act 2015

Audit/reporting
Logs of filtering change controls and of monitoring incidents are made available to:
- the Board of Directors and the Governing Committee
- the Online Safety Coordinator
- the Warwickshire Safeguarding Children's Board, on request

This filtering policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision.

B.3 Personal data security (and transfer)

Please see the School's Data Protection and Retention Policy and the Information Security and Data Breach Policy for more information on the security and transfer of personal data.

Section C. Education

C.1 Online Safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils and other stakeholders in online safety is therefore an essential part of the school's online safety provision. Children and parents need the help and support of the school to recognise and avoid online safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

Online safety education will be provided in the following ways:

- A planned online safety programme should be provided as part of computing, PSHE and other lessons, and should be regularly revisited – this will cover both the use of computer devices and new technologies in school and outside school

- Resources in place relating to the education of online safety are listed in the ICT Policy

- Key online safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises

- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use of computer devices both within and outside school

- In lessons where internet use is pre-planned, it is best practice that pupils 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 pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites visited

- Pupils will be made aware of what to do should they experience anything, while on the internet, which makes them feel uncomfortable

C.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:

    - ✓ Checking the likely validity of the URL (web address).
    - ✓ Cross-checking references (can they find the same information on other sites?)

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils are taught how to make best use of internet search engines to arrive at the information they require

C.3 The contribution of the children to e-learning strategy

It is our general school policy to encourage children to play a contributing role in shaping the way our school operates and this is very much the case with our e-learning strategy.

Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices), could be helpful in their learning.

C.4 Staff training

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:

- All new staff will receive a copy of the Staff Code of Conduct as part of their induction paperwork.
- The Online Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the Department for Education, the local authority, Independent Association of Prep Schools, the Warwickshire Safeguarding Children Board and others
- All teaching staff are able to contribute to the Online Safety Policy via the peer review process
- The Online Safety Coordinator will provide advice, guidance and training as required to individuals on an ongoing basis
- External support for training, including input to parents, is sought regularly from appropriate external providers

C.5 Governor training

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved with digital communications, online safety or child protection. This will usually be through participation in school training/information sessions for staff or parents.

C.6 Parent and carer awareness raising

Many parents and carers may 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 and regulation of the children's online experiences. Parents may often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through letters, newsletters, website, visiting speakers and discussion evenings.