The Croft Preparatory School

E-safety Policy

Whole School Policy, including Early Years Foundation Stage

Section A - Policy and Leadership

This section begins with an outline of the key people responsible for developing our E-safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

A.1.1 Responsibilities: the E-safety Committee

Our school has an E-safety Committee led by the E-safety Coordinator (Ed Bolderston) and made up of teachers and support staff. The E-safety Governor is Anne Freer. The E-safety Committee meets on a termly basis to:

- Review and monitor the E-safety Policy.
- Consider any issues relating to school filtering (see section B.2.1 of this policy).
- Discuss any e-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.1.2 Responsibilities: E-safety Coordinator

Our E-safety Coordinator is Mr Ed Bolderston. He is responsible to the Headmaster and governors for the day-to-day issues relating to the IT infrastructure and e-safety.

The E-safety Coordinator ensures:

- the school's IT infrastructure is secure and is not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in Section B of this policy
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the Headmaster so that appropriate action may be taken

The E-safety Coordinator also:

- leads the E-safety Committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with appropriate external bodies
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- regularly reviews the output from monitoring software and initiates appropriate action where necessary
- considers unblocking requests and instructs CIS to act as appropriate
- meets annually with the E-safety Governor to discuss current issues and review incident logs
- attends relevant meetings of the Governing Committee, as required
- reports regularly to the ELT Meeting and SMT on e-safety matters
- receives appropriate training and support to fulfil his role effectively

A.1.3 Responsibilities: Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out through the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Committee has taken on the role of E-safety Governor which involves:

- annual meetings with the E-safety Coordinator with an agenda based on monitoring of e-safety incident logs
- reporting to Governing Committee meetings

A.1.4 Responsibilities: Headmaster

- The Headmaster is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-safety Coordinator
- The Headmaster and Deputy Headmaster should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in section 2.7 below and relevant HR/disciplinary procedures)

A.1.5 Responsibilities: all 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 e-safety matters and of the current school E-safety Policy and practices
- they have read, understood and signed the school's Acceptable Use Policy for employees
- they report any suspected misuse or problem to the E-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.3.5)
- e-safety issues are embedded in the curriculum and other school activities (see section C)

A.2.1 Policy development, monitoring and review

This E-safety Policy is reviewed by a working group made up of the:

- E-safety Coordinator
- Head of Computing
- Compliance and H&S Manager
- E-safety Governor

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

- Staff meetings
- INSET Days
- Governors' meetings
- Parents' Evenings
- School website

Schedule for development/monitoring/review of this policy

The implementation of this E-safety Policy will be monitored by the:	E-safety Coordinator (Ed Bolderston)
Monitoring will take place at regular intervals:	Once a year
The Governing Committee will receive a report on the implementation of the E-safety Policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually

The E-safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	June 2018
Should illegal e-safety incidents take place, the following external persons / agencies should be informed:	• Warwickshire Safeguarding Children Board e-safety representative • Local Authority Designated Officer • Warwickshire Senior Adviser for Safeguarding Children in Education • Warwickshire Police

A.2.2 Policy Scope

This policy applies to **all members of the school community** (including senior leaders, teaching staff, support staff, pupils, volunteers, 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, 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 e-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 e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use agreements are provided for:

- Pupils (at Year 2, Year 3, and for new entrants to the School in those Year Groups)
- Employees

These agreements are signed by the children and their parents, and by all members of staff.

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. New pupils are provided with an Acceptable Use Agreement as part of their admissions paperwork.

A.2.4 Self-Evaluation

Evaluation of e-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.2.5 Whole School approach and links to other policies

The E-safety Policy has strong links to other school policies as below:

Safeguarding and Child Protection	Safeguarding children electronically is an important aspect of e-safety. ***The E-safety Policy forms a part of the school's overall safeguarding policy.***
Computing Policy	How computing is taught, managed and supported in school.
Internet Acceptable Use Policy Pupils – Year 2	Sets out the principles for safe use of the internet and is signed by both pupils and their parents/carers.
Internet and Email Acceptable Use Policy Pupils – Years 3 - 6	Sets of the principles for safe use of email and the internet and is signed by both pupils and their parents/carers.
Mobile Device Agreement and Acceptable Use Policy	Relates to the safe use of mobile devices by members of staff.
Password Policy	How passwords should be set and managed to ensure IT security within the School.
Internet and Email Acceptable Use Policy for Employees	Outlines expectations and safe internet and email usage for employees.
Twitter Policy	Outlines expectations and safe use of Twitter by staff to promote pupil activities and the school

Other policies relating to E-safety

Anti-bullying	How the school strives to eliminate bullying and cyberbullying.
PSHE	E-safety has links to staying safe.
Good Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.

A.2.6 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 (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – 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 ICT 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 more likely 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 as follows:

Pupil sanctions *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Refer to class teacher	Refer to E-safety Coordinator	Refer to Headmaster	Refer to Police	Refer to E-safety Coordinator for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔				✔	✔	✔	✔	
Unauthorised use of mobile phone / digital camera / other handheld device	✔		✔						
Unauthorised use of social networking / instant messaging / personal email	✔				✔			✔	
Unauthorised downloading or uploading of files	✔						✔		
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	

Pupil Sanctions continued/…

	Refer to class teacher	Refer to E-safety Coordinator	Refer to Headmaster	Refer to Police	Refer to E-safety Coordinator for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Attempting to access the school network, using another pupil's account	✔								
Attempting to access or accessing the school network, using the account of a member of staff	✔		✔		✔	✔		✔	
Corrupting or destroying the data of other users	✔				✔	✔	✔	✔	
Sending an email, text or instant message or posting information online that is regarded as defamatory, offensive, harassment or of a bullying nature	✔	✔	✔			✔	✔	✔	✔
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔	✔	✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔		✔						
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔							
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔						

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 if the incident is deemed to be malicious and harmful to either an individual staff member or the school as a whole.

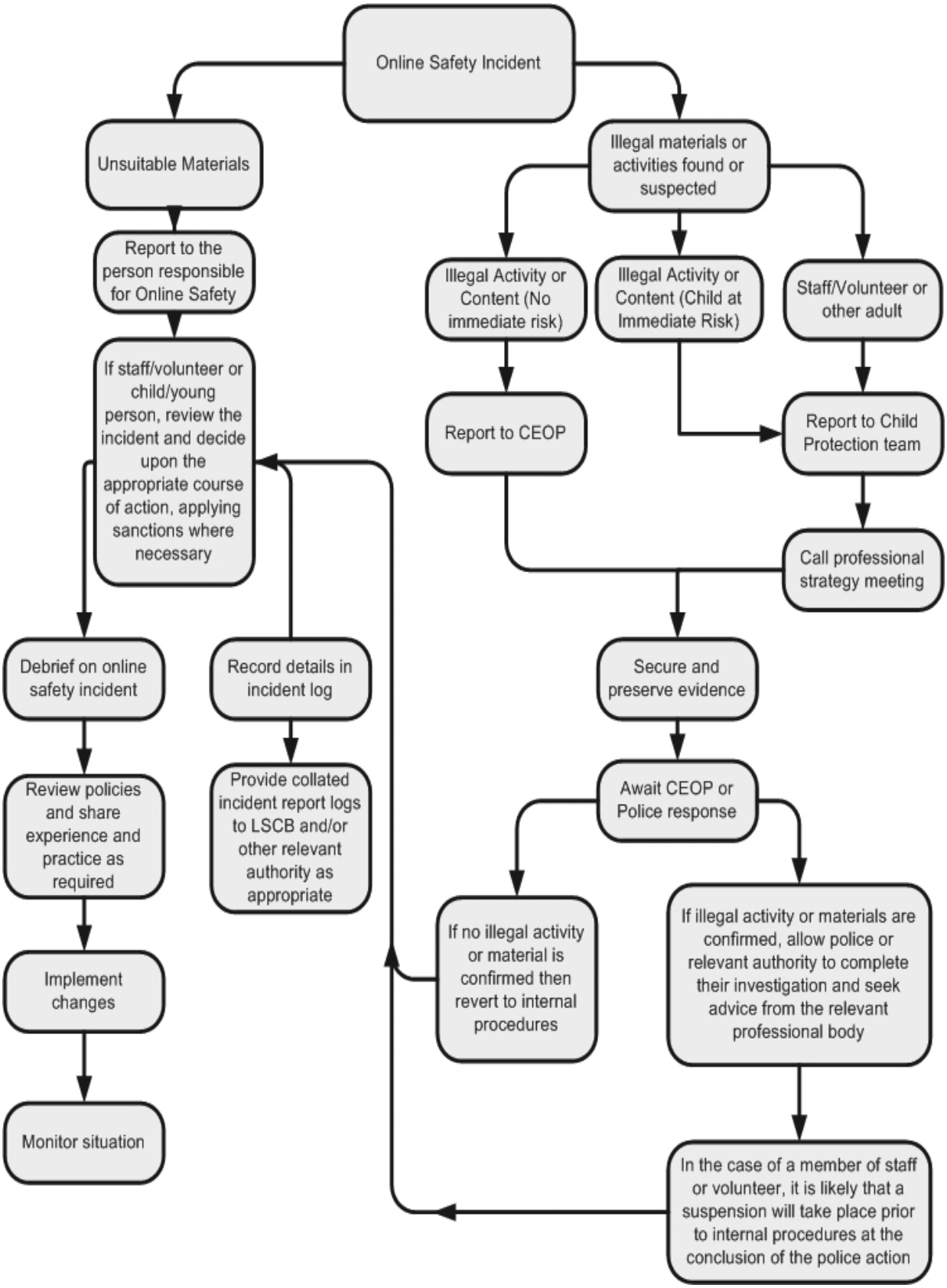
Staff sanctions *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Refer to Line Manager	Refer to Headmaster	Refer to Local Authority / HR	Refer to Police	Refer to E-safety Coordinator for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		✔	✔	✔			✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		✔
Unauthorised downloading or uploading of files	✔				✔	✔		✔
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔	✔			✔	✔		✔
Careless use of personal data eg holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	✔
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message or posting information online that is regarded as defamatory, offensive, harassment or of a bullying nature	✔	✔				✔	✔	✔
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✔	✔						
Actions which could compromise the staff member's professional standing	✔	✔						

Staff sanctions continued/…	Refer to Line Manager	Refer to Headmaster	Refer to Local Authority / HR	Refer to Police	Refer to E-safety Coordinator for action re filtering etc	Warning	Suspension	Disciplinary action
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔	✔				✔		✔
Using proxy sites or other means to subvert the school's filtering system	✔	✔			✔	✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔						
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔			✔	✔	✔
Breaching copyright or licensing regulations	✔	✔						
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

A.2.7 Reporting of E-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, 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.2.6 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.3.1 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, 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 and not held on the employee (eg in an apron pocket) unless on the express permission of the Early Years Manager.
- Personal mobile phones should never be used for contacting parents, except in an emergency.
- 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 DSP 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.

	Staff / adults				**Pupils**			
Personal handheld technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	✔							✔
Use of mobile phones in lessons		✔						✔
Use of mobile phones in social time	✔							✔
Taking photos of children in school on personal phones or other camera devices				✔				✔
Use of handheld devices e.g. gaming consoles		✔						✔

A.3.2 Use of communication technologies

A.3.2a – Email

Access to email is provided for all employees and all pupils from Year 3 upwards using their personal login details.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- 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/E-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.

	Staff / adults				**Pupils**			
Use of Email	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of personal email accounts in school / on school network		✔						✔
Use of school email for personal emails				✔				✔

A.3.2b - Social networking (including chat, Twitter, instant messaging, blogging etc)

	Staff / adults				Pupils			
Use of social networking tools	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non-work related chat rooms				✔				✔
Use of personal Twitter account				✔				✔
Use of non-work related instant messaging				✔				✔
Use of non-work related social networking sites				✔				✔
Use of non-work related blogs				✔				✔

A.3.3 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.3.4) for guidance on publication of photographs.

A.3.4 Use of web-based publication tools

A.3.4a - 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.3.5 Professional standards for staff communication

In all aspects of their work teachers abide by The Croft Preparatory School Teachers' Standards. Teachers translate these standards appropriately for all matters relating to e-safety.

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, Twitter accounts, 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.

B.2.1 Filtering

B.2.1a - 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.

B.2.1b - Responsibilities

Overall responsibility for the management of the school's filtering policy is held by the E-safety Coordinator (with ultimate responsibility resting with the Headmaster and Governing Committee). Day to day management of the school filtering, in line with this policy, is carried out by the School's external IT support services, on instruction by the E-safety Coordinator.

To ensure that there is a system of checks and balances, and to protect those responsible, changes to the school filtering service must be authorised by the Executive Leadership Team (ELT).

All users have a responsibility to report immediately to class teachers/E-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.

B.2.1c - Education/training/awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme (see section C of this policy).

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

- signing the Acceptable Use Agreement for Employees (a part of their induction process)
- 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 Agreements.

B.2.1d - 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 technical support via the following email address: TechSupport@ciservice.co.uk

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 E-safety Coordinator will be responsible for considering all requests and instructing external technicians to sanction the unblocking or otherwise.

B.2.1e – 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 E-safety Coordinator reviews the Impero console captures 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 pupil's use of the internet in accordance with 'The Prevent Duty Guidance' relating to the Counter-Terrorism and Security Act 2015

B.2.1f - Audit/reporting

Logs of filtering change controls and of monitoring incidents are made available to:

- the E-safety Governor
- the E-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.2.2 Personal data security (and transfer)

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

Section C. Education

C.1.1 E-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 e-safety is therefore an essential part of the school's e-safety provision. Children and parents need the help and support of the school to recognise and avoid e-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.

E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PSHE and other lessons, and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Resources in place relating to the education of e-safety are listed in the ICT Policy.
- Key e-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 ICT 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 the young people visit.
- Pupils will be made aware of what to do should they experience anything, while on the internet, which makes them feel uncomfortable.

C.1.2 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.1.3 The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading 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.2 Staff training

It is essential that all staff receive e-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 E-safety Policy and Acceptable Use Policy for Employees as part of their induction paperwork. The Acceptable Use Policy should be signed and returned to the HR Department.
- The E-safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, IAPS, the WSCB and others.
- All teaching staff are able to contribute to the E-Safety Policy via the peer review process.
- The E-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.3 Governor training

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

The E-safety Governor works closely with the E-safety Coordinator and reports back to the full Governing Committee (see section A.1.3)

C.4 Parent and carer awareness raising

Many parents and carers may have only a limited understanding of e-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.

Appendix 1 - Glossary of terms

CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
DfE	Department for Education
IAPS	The Independent Association of Prep Schools
ICT	Information and Communications Technology
Impero	Remote monitoring and managing software
INSET	In Service Education and Training
Learning platform	An online system designed to support teaching and learning in an educational setting
PSHE	Personal, Social and Health Education
URL	Universal Resource Locator – a web address
WSCB	Warwickshire Safeguarding Children Board (the local safeguarding board)

Policy review	June 2017
Peer Review completed	30 June 2017
Approved ELT	10 July 2017
Review	June 2018