

THE CEDAR FEDERATION

Ifield School & King's Farm Primary School

Online Safety Policy

Date: Summer 2018

Review Date: Summer 2019



**Children, Young People and Education
Directorate**

Education Safeguarding Team

The Cedar Federation

Ifield School and King's Farm Primary School

Key Details

Designated Safeguarding Leads:

Ifield School

Miss Madeleine Jones – Head of School

King's Farm Primary School

Mr Chris Jackson – Head of School

Deputy Designated Safeguarding Leads:

Ifield School

Mrs Abigail Birch – Executive Headteacher

Mr Sam Kelleher – Assistant Headteacher

Mrs Sam Hargood – Sixth Form Teaching, Learning & Curriculum Lead

Mr Paul Jackson – Deputy Director

Miss Denise Moore – Head of Sixth Form

King's Farm Primary School

Mrs Abigail Birch – Executive Headteacher

Mrs Kim Mitten – Family Support

Mr Paul Jackson – Deputy Director

Named Governor with lead responsibility:

Mr Andrew Sparks

Date written: (October, 2017) Updated: (May 2018)

Date agreed and ratified by Governing Body: (Summer 2018)

Date of next review: (Summer, 2019)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

	Page no
1. Policy Aims	5
2. Policy Scope	5
2.2 Links with other policies and practices	5
3. Monitoring and Review	6
4. Roles and Responsibilities	6
4.1 The leadership and management team	6
4.2 The Designated Safeguarding Lead	7
4.3 members of staff	7
4.4 Staff who manage the technical environment	8
4.5 Pupils	8
4.6 Parents	9
5. Education and Engagement Approaches	9
5.1 Education and engagement with pupils	9
5.2 Training and engagement with staff	10
5.3 Awareness and engagement with parents	11
6. Reducing Online Risks	11
7. Safer Use of Technology	12
7.1 Classroom Use	12
7.2 Managing Internet Access	13
7.3 Filtering and Monitoring	14
7.4 Managing Personal Data Online	15
7.5 Security and Management of Information Systems	15
7.6 Managing the Safety of the School Website	16
7.7 Publishing Images and Videos Online	16
7.8 Managing Email	16
7.9 Educational use of Videoconferencing and/or Webcams	17
7.10 Management of Learning Platforms	
7.11 Management of Applications (apps) used to Record Children's Progress	18
8. Social Media	19
8.1 Expectations	19
8.2 Staff Personal Use of Social Media	19
8.3 Pupils' Personal Use of Social Media	20
8.4 Official Use of Social Media	22
9. Use of Personal Devices and Mobile Phones	22
9.1 Expectations	22
9.2 Staff Use of Personal Devices and Mobile Phones	22
9.3 Pupils' Use of Personal Devices and Mobile Phones	23
9.4 Visitors' Use of Personal Devices and Mobile Phones	24
9.5 Officially provided mobile phones and devices	24
10. Responding to Online Safety Incidents and Concerns	24
10.1 Concerns about Pupils Welfare	25
10.2 Staff Misuse	25
11. Procedures for Responding to Specific Online Incidents or Concerns	26
11.1 Youth Produced Sexual Imagery or "Sexting"	26
11.2 Online Child Sexual Abuse and Exploitation	27
11.3 Indecent Images of Children (IIOC)	28
11.4 Cyberbullying	29
11.5 Online Hate	30
11.6 Online Radicalisation and Extremism	30
12. Useful Links for Educational Settings	32

The Cedar Federation Online Safety Policy

1. Policy Aims

- This online safety policy has been written by The Cedar Federation, involving staff, pupils and parents/carers, building on the Kent County Council (KCC) online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance “[Keeping Children Safe in Education](#)” 2016, [Early Years and Foundation Stage](#) 2017 and the [Kent Safeguarding Children Board](#) procedures.
- The purpose of The Cedar Federation online safety policy is to:
 - Safeguard and protect all members of The Cedar Federation community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns.
- The Cedar Federation identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
 - **Content:** being exposed to illegal, inappropriate or harmful material
 - **Contact:** being subjected to harmful online interaction with other users
 - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

2. Policy Scope

- The Cedar Federation believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all pupils and staff are protected from potential harm online.
- The Cedar Federation identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Cedar Federation believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets, mobile phones and cameras.

2.2 Links with other policies and practices

- This policy links with a number of other policies, practices and action plans including:
 - Anti-bullying policy
 - Acceptable Use Policies (AUP) and the Code of conduct
 - Behaviour and wellbeing policy
 - Safeguarding and Child protection policy
 - Confidentiality policy

- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Data protection policy
- Photographic Image use policy
- Searching, screening and confiscation policy
- Staff supervision policy
- Whistleblowing policy

3. Monitoring and Review

- The Cedar Federation will review this policy at least annually
 - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Executive Headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

4. Roles and Responsibilities

- The schools have appointed Miss Madeleine Jones (Ifield) and Mr Chris Jackson (King's Farm), as Designated Safeguarding Leads to be the online safety lead.
- The Cedar Federation recognises that all members of the community have important roles and responsibilities to play with regards to online safety.
- The Cedar Federation has a duty to provide the Federation community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.

4.1 The leadership and management team will:

- Ensure that online safety is viewed by the Federation community as a safeguarding issue and that practice is in line with national and local recommendations and requirements to proactively develop a robust online safety culture.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a Code of conduct and/or an AUP, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place.
- Work with technical staff to monitor the safety and security of school systems and networks.
- Ensure that online safety is embedded within a progressive whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the Designated Safeguarding Lead by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.

- Ensure there are robust reporting channels for the school community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology including ensuring the safe and responsible use of devices. Audit and evaluate online safety practice to identify strengths and areas for improvement.
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.

4.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the school community, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and provide guidance regarding safe appropriate communications.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly (**Termly**) with the governor with a lead responsibility for safeguarding and/or online safety.
- Be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- Ensure that online safety is integrated with other appropriate school policies and procedures.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and AUPs..
- Take responsibility for the security of school systems and the data they use, or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.

- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Demonstrate an emphasis on positive learning opportunities.

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures to provide a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- Implement appropriate security measures (*including access control, password policies and encryption*) to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that the schools filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL and leadership team, as well as, the school's Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL, in accordance with the school's safeguarding procedures.
- Develop an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- Provide technical support and perspective to the DSL and Leadership Team, especially in the development and implementation of appropriate online safety policies and procedures.
 - Ensuring that the school's IT infrastructure/system is secure and not open to misuse or malicious incidents.
 - Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
 - Ensuring that appropriately strong passwords are applied and enforced for all.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the school AUPs.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.

- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the school AUPs and encourage their children to adhere to them and adhere to them themselves.
- Support the school in their online safety approaches by discussing online safety issues with their children and reinforce appropriate, safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the school's home-school agreement and/or AUPs. Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the school online safety policies.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- The school will establish and embed a progressive online safety curriculum throughout the whole school, to raise awareness and promote safe and responsible internet use amongst pupils by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in the PSHE, RSE and Computing programmes of study, covering use both at school and home. (SMSC Policy, Behaviour & Wellbeing Policy, SRE Policy, Safer Internet Day, Acceptable Use Statements, Online Policy, Safeguarding and Child Protection Policy)
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will support pupils to read and understand the AUP in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology by pupils.
 - Implementing appropriate peer education approaches as appropriate to the needs of the pupils. (*e-safety ambassadors*)
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.

- Seeking pupil voice when writing and developing school online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support the schools internal online safety education approaches.

5.1.1 Vulnerable Pupils

- The Cedar Federation is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The Cedar Federation will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. The curriculum is highly personalised, differentiated and adapted according to individual pupils needs. Acceptable Use Statements are available in symbol format to aid communication
- The Cedar Federation will seek input from specialist staff as appropriate, including the SENCO, Child in Care Lead, Teaching, Learning and Curriculum Lead, DSO.
- The school filtering system Netsupport DNA filters words from different languages.

5.2 Training and engagement with staff

The schools will:

- Provide and discuss the online safety policy with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates. (*annual training, termly safeguarding updates*)
 - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

5.3 Awareness and engagement with parents and carers

- The Cedar Federation recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
 - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
 - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.
 - Requiring them to read the school AUP and discuss its implications with their children.

6. Reducing Online Risks

- The Cedar Federation recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:
 - Regularly review the methods used to identify, assess and minimise online risks.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via a school computer or device.
- All members of the school community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in the school's AUP and highlighted through a variety of education and training approaches.
- The Federation will audit technology use to establish if the Online Safety Policy is adequate and that the implementation of the policy is appropriate.
- The Federation will ensure that appropriate filtering and monitoring systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. The current filtering system at Ifield and King's Farm School is LightSpeed and Netsupport DNA which monitors all web traffic. Access to the internet at the Link Centre, North Kent College is filtered via Forti Gate. The Cedar Federation liaises with North Kent College to ensure the level of filtering is appropriate.

Internet use throughout the wider school

- The Cedar Federation will liaise with local organisations to establish a common approach to online safety.
- The Cedar Federation will work with the local community's needs (including recognising cultural backgrounds, languages, religions and ethnicity) to ensure internet use is appropriate.
- The Cedar Federation will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

- Internet use is a key feature of educational access and all pupils will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access specific curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard pupils and supervision, classroom management and education about safe and responsible use is essential.

Authorising internet access

- The Cedar Federation will maintain a current record of all staff and pupils who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign the Acceptable Use Policy before using any school resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- The use of tablets within the Federation is increasing. Access to the internet can be disabled or enabled on an individual basis as decided by the teacher. All pupils using tablets are supervised and the filtering system works effectively.

7. Safer Use of Technology

7.1 Classroom Use

- The Cedar Federation uses a wide range of technology. This includes access to: (*this list is not exhaustive*)
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - School learning platform/intranet
 - Email
 - Games consoles and other games based technologies
 - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with the school's AUP and with appropriate safety and security measures in place. (*Acceptable use policy, adult supervision, passwords and filtering*)
- The school uses Lightspeed & Netsupport DNA webfiltering, the LINK Centre uses Forti Gate webfiltering to protect users online within school on all devices and Zulu Desk to enforce tablet restrictions on what can be accessed.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools (Puffin Academy *and* Google Safe Search), following an informed risk assessment, to identify which tool best suits the needs of our community.
- The school will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Supervision of pupils will be appropriate to their age and ability.
 - **Early Years Foundation Stage and Key Stage 1**
 - Pupils' access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils' age and ability.
 - This will be supervised by an adult at all times.
 - **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
 - This will be supervised by an adult at all times.
 - **Key Stage 3, 4,**
 - Pupils will be appropriately supervised when using technology, according to their ability and understanding.
 - **Key Stage 5**
 - Pupils will be appropriately supervised when using technology, according to their ability and understanding.
 - The school will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).
 - **Field Life**
 - Pupils will be appropriately supervised when using technology, according to their ability and understanding.
 - The school will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children in accordance with the national minimum standards (NMS).

7.2 Managing Internet Access

- The school will maintain a written record of users who are granted access to the school's devices and systems.
- All staff, pupils and visitors will read and sign an AUP before being given access to the school computer system, IT resources or internet.

7.3 Filtering and Monitoring

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: <https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>

The school's internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.

All monitoring of school owned/provided systems will take place to safeguard members of the community.

7.3.1 Decision Making

- The Cedar Federation governors and leaders have ensured that the school has age and ability appropriate filtering and monitoring in place, to limit children's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what children can be taught, with regards to online activities and safeguarding.
- The school's decision regarding filtering and monitoring has been informed by a risk assessment, taking into account our school's specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

7.3.2 Filtering

- The school uses educational broadband connectivity through KPSN which is appropriate to the age and requirement of our pupils. (EIS)
- The school uses Lightspeed & Netsupport DNA webfiltering, the LINK Centre uses Forti Gate webfiltering to protect users online within school on all devices and Zulu Desk to enforce tablet restrictions on what can be accessed which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming, offensive language and sites of an illegal nature.
 - The school filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
 - The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
 - Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
 - All changes to the school filtering policy will be logged and recorded.
- The school works with KCC and the schools Broadband Team (EIS) to ensure that our filtering policy is continually reviewed.

Dealing with Filtering breaches

- The school has a clear procedure for reporting filtering breaches which all members of the Federation community are aware of.
 - If pupils or staff discover unsuitable sites, they will be required to report the URL to the DSL which will then be recorded and escalated as appropriate (e.g. turn off monitor/screen and report the concern immediate to a member of staff).
 - The member of staff will report the concern (including the URL of the site if possible) to the Designated Safeguarding Lead and/or technical staff.
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Kent Police or CEOP.

7.3.4 Monitoring

- The schools will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
 - This will be achieved e.g. physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.
- The school has a clear procedure for responding to concerns identified via monitoring approaches. DSL will respond in line with the Safeguarding and Child Protection Policy.
- All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with the Data Protection Act 1998.
 - Full information can be found in the schools information security Data Protection policy.

7.5 Security and Management of Information Systems

- The school takes appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.
 - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
 - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
 - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
 - Regularly checking files held on the school's network,
 - The appropriate use of user logins and passwords to access the school network.
 - Specific user logins and passwords will be enforced for all but the youngest users. (For Early Years and Foundation Stage children)
 - All users are expected to log off or lock their screens/devices if systems are unattended.

- Further information about technical environment safety and security can be found at in the School's Acceptable Use Policy, Staff Handbook, Code of Conduct and Child Protection Policy.)

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access school systems; members of staff are responsible for keeping their password private.
- From year R all pupils are provided with their own unique username and private passwords to access school systems; pupils are responsible for keeping their password private.
- We require all staff users to:
 - Use strong passwords for access into our system.
 - Change their passwords every <6 months.
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

7.6 Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

7.7 Publishing Images and Videos Online

- The school will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to): the Photographic Image Use Policy, Data Protection Policy, AUPs, Codes of conduct, Social media and Use of personal devices and mobile phones.
- In line with the Photographic Image Use Policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

7.8 Managing Email

- Access to school email systems will always take place in accordance with Data protection legislation and in line with other school policies, including: Confidentiality, AUPs and Code of conduct.
 - The forwarding of any chain messages/emails is not permitted. Spam or junk mail will be blocked and reported to the email provider.

- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the school community will immediately tell (Head of School) if they receive offensive communication, and this will be recorded in the school safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked in school.
- Access to school email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. Data Protection.

7.8.1 Staff

- The use of personal email addresses by staff for any official school business is not permitted.
 - All members of staff are provided with a specific school email address, to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent internally using secure and encrypted email. Any external emails sent sharing sensitive or personal information will be password protected.

7.8.2 Pupils

- Pupils will use school provided email accounts for educational purposes.
- Pupils will sign an AUP and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the school.

7.9 Educational use of Videoconferencing and/or Webcams

- The Cedar Federation recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.
 - All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.
 - Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
 - Videoconferencing contact details will not be posted publically.
 - School videoconferencing equipment will not be taken off school premises without prior permission from the DSL.
 - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

7.9.1 Users

- Parents and carers consent will be obtained prior to pupils taking part in videoconferencing activities.
- Pupils will ask permission from a teacher before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the pupils' age and ability by constant adult supervision, appropriate checks being made of the proposed conferencing.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

7.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, the school will check that recording is permitted to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-school site, staff will check that the material they are delivering is appropriate for the class.

7.10 Management of Learning Platforms

- Ifield School uses Tapestry as an official learning platform to record PE Enrichment progress.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, in particular, message and communication tools and publishing facilities.
- Only current members of staff, pupils and parents will have access to the LP.
- When staff and/or pupils' leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Pupils and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:
 - The user will be asked to remove any material deemed to be inappropriate or offensive.
 - If the user does not comply, the material will be removed by the site administrator.
 - Access to the LP for the user may be suspended.
 - The user will need to discuss the issues with a member of leadership before reinstatement. A pupil's parent/carer may be informed.
 - If the content is considered to be illegal, then the school will respond in line with existing child protection procedures.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

7.11 Management of Applications (apps) used to Record Children's Progress

- The school uses Pupil Asset and Tapestry to track pupils progress and share appropriate information with parents and carers.
- The Executive Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation
- In order to safeguard pupils data:
 - Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
 - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
 - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
 - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
 - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of The Cedar Federation community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of The Cedar Federation community are expected to engage in social media in a positive, safe and responsible manner, at all times.
 - All members of The Cedar Federation community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- The school will control pupil and staff access to social media whilst using school provided devices and systems on site by training and filtering.
 - The use of social media during school hours for personal use **is not** permitted.
 - Both schools have blocked pupil and staff access to social media and social networking sites whilst on site and when using school provided devices and systems
 - Inappropriate or excessive use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of The Cedar Federation community on social media, should be reported to the school and will be managed in accordance with our Anti-bullying, Allegations against staff, Behaviour and Child protection policies.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be in accordance with relevant policies, such as anti-bullying, managing allegations against staff, behaviour & wellbeing and safeguarding/child protection.

8.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of the school Code of conduct within the AUP.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within school. Civil, legal or disciplinary action may be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - Setting the privacy levels of their personal sites as strictly as they can.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of The Cedar Federation on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members.
 - Members of staff will ensure that they do not represent their personal views as that of the school on social media.
 - The Cedar Federation email addresses will not be used for setting up personal social media accounts.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with schools policies and the wider professional and legal framework.
 - Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role in the school.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or current or past pupils' family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this will be discussed with Designated Safeguarding Lead and/or the Executive Headteacher.
 - If ongoing contact with pupils is required once they have left the school roll, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to make contact with pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Executive Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the schools Designated Safeguarding Lead.
- All communication between staff and members of the school community on school business will take place via official approved communication channels such as an official setting provided email address or phone numbers.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- The school is aware that many popular social media sites state that they are not for children under the age of 13, therefore the school will not create accounts specifically for children under this age.
- Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.
- Pupils will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, other social media contact details, email addresses, full names of friends/family, specific interests and clubs.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private/protected.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications and report concerns both within school and externally.
- Personal publishing on social media sites will be taught to pupils as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.

- Pupils will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs.
- Pupils will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Parents will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- Any official social media activity involving pupils will be moderated by the school where possible.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Any concerns regarding pupils' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

8.4 Official Use of Social Media

- *King's Farm Primary School* official social media channels are:
 - **Facebook**
- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Executive Headteacher.
 - Leadership staff have access to account information and login details for the social media channels, in case of emergency, such as staff absence.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use school provided email addresses to register for and manage any official school social media channels.
 - Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
 - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: Anti-bullying, Image use, Data protection, Confidentiality and Safeguarding and child protection.

- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents, carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - *Social media tools which have been risk assessed and approved as suitable for educational purposes will be used.*
- Parents and carers will be informed of any official social media use with pupils and written parental consent will be obtained, as required.
- The school will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like the school social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Sign the school's Social media acceptable use policy.
 - Be professional at all times and aware that they are an ambassador for the school.
 - Disclose their official role and/or position, but make it clear that they do not necessarily speak on behalf of the school.
 - Be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: Libel, Defamation, Confidentiality, Copyright, Data protection and Equalities laws.
 - Ensure that they have appropriate written consent before posting images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, pupils, parents and carers.
 - Inform their line manager, the Designated Safeguarding Lead and/or the Executive Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

9. Use of Personal Devices and Mobile Phones

The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members community to take steps to ensure that mobile phones, cameras and personal devices are used responsibly.

The use of mobile phones, cameras and other personal devices by young people and adults will be decided by the school and is covered in appropriate policies including the school Acceptable Use Policy.

- The Cedar Federation recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Photographic Image Use, Acceptable Use Policy, Staff Handbook, Safeguarding and Child Protection Policy, Anti-bullying, Behaviour and Child protection. Electronic devices of any kind that are brought onto site are the responsibility of the user at all times.
 - All members of The Cedar Federation community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; the school accepts no responsibility for the loss, theft or damage of such items on school premises.
 - All members of The Cedar Federation community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the school site such as changing rooms, toilets, personal care rooms, Ifield Life, Early Years Classrooms and swimming pools.
- The sending of abusive or inappropriate messages/ content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our Behaviour policy.
- All members of The Cedar Federation community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school Behaviour or Child protection policies.

9.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones, cameras and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Online Safety, Data Protection, Safeguarding and Child protection, Acceptable use policies and the staff handbook.
- Staff will be advised to:
 - Keep mobile phones, cameras and personal devices in a safe and secure place during lesson time.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless written permission has been given by the Head of School / Executive Headteacher, such as in emergency circumstances.
 - Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead and/or Executive Headteacher.
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.

- Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school behaviour and allegations policy
 - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

9.3 Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices, cameras and mobile phones and will be made aware of boundaries and consequences.
 - Pupils should protect their phone numbers by only giving them to trusted friends and family members.
 - Pupils will be instructed in safe and appropriate use of mobile phones, cameras and personal devices and will be made aware of boundaries and consequences.
- The Cedar Federation expects pupil's personal devices and mobile phones to be handed to the class teacher or office staff at the start of the school day. 6th Form?
- If a pupil needs to contact his/her parents or carers they will be allowed to use a school phone.
 - Parents are advised to contact their child via the school office during school hours; exceptions may be permitted on a case-by-case basis, as approved by the Head of School. 6th form?
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of the Leadership Team.
 - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
 - If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
 - Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place.
 - School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the school's Behaviour or Bullying policy, or could contain youth produced sexual imagery (sexting).
 - The phone, camera or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone, cameras or personal devices will only be carried out in accordance with the schools policy.
 - Searches of mobile phone or personal devices will only be carried out in accordance with the school's policy. (Behaviour and wellbeing policy)
www.gov.uk/government/publications/searching-screening-and-confiscation
 - Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes school policies.

- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

9.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.
- Use of mobile phones, cameras or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.

9.5 Officially provided mobile phones and devices.

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
 - Pupils, parents and staff will be informed of the school's complaints procedure and staff will be made aware of the whistleblowing procedure.
- The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, the school will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.

- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with Kent Police and/or the Education Safeguarding Team first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils Welfare

- The DSL will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL will record these issues in line with the school's child protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Executive Headteacher, according to the Allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with the Behaviour policy and Code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Youth Produced Sexual Imagery or “Sexting”

- The Cedar Federation recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; therefore all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches via a range of age and ability appropriate educational approaches for pupils, staff and parents/carers. (Identify resources as appropriate).
- The Cedar Federation views “sexting” as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead (Miss Madeleine Jones – Ifield or Mr Chris Jackson – King’s Farm).
- The school will follow the guidance as set out in the non-statutory UKCCIS advice ‘Sexting in schools and colleges: responding to incidents and safeguarding young people’ and KSCB “Responding to youth produced sexual imagery” guidance
- The school will follow the advice as set out in the non-statutory UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and [KSCB](#) guidance: “Responding to youth produced sexual imagery”.
- The Cedar Federation will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods such as Online Safety Curriculum, Online safety ambassadors, internal and external training.
- The school will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.1.1 Dealing with ‘Sexting’

- If the school are made aware of an incident involving the creation or distribution of youth produced sexual imagery, the school will:
 - Act in accordance with our Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board’s procedures.
 - Immediately notify the Designated Safeguarding Lead.
 - Store the device securely.
 - If an indecent image has been taken or shared on the school network or devices, the school will take action to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of pupil(s) involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Specialist Children’s Services and/or the Police, as appropriate.
 - Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
 - Consider the vulnerabilities of pupil (s) involved (including carrying out relevant checks with other agencies)

- Implement appropriate ~~sanctions~~ next steps in accordance with the school's Behaviour policy, but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: ['Sexting in schools and colleges: responding to incidents and safeguarding young people'](#) guidance.
 - Images will only be deleted once the school has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.
- The school will take action regarding youth produced sexual imagery, regardless of whether the incident took place on/off school premises, using school or personal equipment.
- The school will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - In this case, the image will only be viewed by the Designated Safeguarding Lead and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of children (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.
- If an indecent image has been taken or shared on the school network or devices then the school will take action to block access to all users and isolate the image.
- The Cedar Federation will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- The Cedar Federation will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.

11.2 Online Child Sexual Abuse and Exploitation

- The Cedar Federation will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The Cedar Federation recognises online child sexual abuse as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate education for pupils, staff and parents/carers.
- The school will ensure that all members of the community are aware of the support available regarding online child sexual abuse, both locally and nationally.
- The school will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of the school community on the school website.

11.2. 1 Dealing with Online Child Sexual Abuse and Exploitation

- If the school are made aware of incident involving online sexual abuse of a child, the school will:
 - Act in accordance with the school's Child protection and Safeguarding policies and the relevant Kent Safeguarding Child Board's procedures.
 - Immediately notify the Designated Safeguarding Lead.

- Store any devices involved securely.
- Immediately inform Kent police via 101 (or 999 if a child is at immediate risk)
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Make a referral to Specialist Children's Services (if required/ appropriate).
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; school leadership team will review and update any management procedures, where necessary.
- The school will take action regarding online child sexual abuse, regardless of whether the incident took place on/off school premises, using school or personal equipment.
 - Where possible pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report :
www.ceop.police.uk/safety-centre/
- If the school is unclear whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the Designated Safeguarding Lead.
- If pupils at other schools are believed to have been targeted, the school will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.3 Indecent Images of Children (IIOC)

- The Cedar Federation will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- The school will take action regarding IIOC on school equipment and/or personal equipment, even if access took place off site.
- The school will take action to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If the school is unclear if a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, the school will:
 - Act in accordance with the schools child protection and safeguarding policy and the relevant Kent Safeguarding Child Boards procedures.
 - Immediately notify the school Designated Safeguard Lead.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children whilst using the internet, the school will:

- Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school devices, the school will:
 - Ensure that the Designated Safeguard Lead is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school devices, the school will:
 - Ensure that the Head of School / Executive Headteacher is informed.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
 - Quarantine any devices until police advice has been sought.
 - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
 - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
 - Follow the appropriate school policies regarding conduct.

11.4 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at The Cedar Federation.
- Full details of how the school will respond to cyberbullying are set out in the Anti-bullying policy.
- All incidents of online bullying reported will be recorded.
- There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.
- Pupils, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
 - Sanctions for those involved in online or cyberbullying may include:
 - Those involved will be asked to remove any material deemed to be inappropriate or offensive.
 - A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
 - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
 - Parent/carers of pupils involved in online bullying will be informed.
 - The Police will be contacted if a criminal offence is suspected.

11.5 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated by The Cedar Federation and will be responded to in line with existing school policies, including Anti-bullying and Behaviour.
- All members of the community will be advised to report online hate in accordance with relevant school policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If the school is unclear on how to respond, or whether a criminal offence has been committed, the Designated Safeguarding Lead will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.6 Online Radicalisation and Extremism

- The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school through the school's Prevent Curriculum, British Values teaching and the Filtering system.
- If the school is concerned that a child or parent/carer may be at risk of radicalisation online, the Designated Safeguarding Lead will be informed immediately and action will be taken in line with the Safeguarding and Child protection policy.
- If the school is concerned that member of staff may be at risk of radicalisation online, the Executive Headteacher will be informed immediately and action will be taken in line with the Child protection and Allegations policies.
- The school will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. A filtering report is configured to alert us if any web search is carried out on these blocked categories.
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.

- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or Kent Police.

Whistleblowing

All staff and volunteers should feel able to raise concerns about poor or unsafe practice and such concerns will always be taken seriously by the senior leadership team.

- All members of staff are made aware of the school's Whistle-blowing procedure and that it is a disciplinary offence not to report concerns about the conduct of a colleague that could place a child at risk.
- Members of Staff can also access the NSPCC whistleblowing helpline if they do not feel able to raise concerns regarding child protection failures internally. Staff can call: 0800 028 0285 (8:00 AM to 8:00 PM Monday to Friday) or email: help@nspcc.org.uk

12. Useful Links for Educational Settings

Kent Support and Guidance

Kent County Council Education Safeguarding Team:

- Rebecca Avery, Education Safeguarding Adviser (Online Protection)
- Ashley Assiter, e-Safety Development Officer
 - esafetyofficer@kent.gov.uk Tel: 03000 415797
- Guidance for Educational Settings:
 - www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding
 - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
 - www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
 - Kent e–Safety Blog: www.kentesafety.wordpress.com

KSCB:

- www.kscb.org.uk

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101

Other:

- Kent Public Service Network (KPSN): www.kpsn.net
- EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

Single Equalities Scheme impact Assessment (Equalities Act 2010)

This policy has been developed to ensure that there is no negative or adverse impact on any individual or group in terms of disability, race, belief, gender, sexual orientation or age. All opportunities for potential positive impact on individuals, groups and the community are embedded within the ethos, vision and values of the school.

The Cedar Federation is committed to achieving Best Value in all decisions made. We use the principles of Best Value as they apply to securing continuous improvement in the Federation.

Date: Summer 2018

Review Date: Summer 2019

Signed by Chair of Governors:.....

Signed by Chair of Teaching, Learning and Assessment Committee:

Signed by Executive Headteacher:.....



Ifield School Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 6 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly every 60 days).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Network Manager, Mr Michael Sims.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN/DirectAccess). Any images or videos of pupils will only be used as stated in the school image use policy ([Photographic Image Use Policy](#)) and will always take into account parental consent.
7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops,

digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use staff drives to upload any work documents and files in a password protected environment via VPN/DirectAccess. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will respect copyright and intellectual property rights.
10. I have read and understood the school Online Safety Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces, ([Online Safety Policy](#))
11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead, Maddy Jones immediately. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Maddy Jones, Designated Safeguarding Lead and/or the designated lead for filtering, Michael Sims immediately.
12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead, Michael Sims.
13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head of School.
14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.
15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
16. I will promote online safety with the pupils in my care and will support them to develop a responsible attitude to safety online, system use and to the content they access or create.
17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead, Maddy Jones.
18. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

19. I understand that mobile phones and personal devices are not permitted to be used in certain areas within the school such as changing rooms, personal care rooms, toilets, Ifield Life and the hydro pool.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:

Dear Staff Member,

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be “private” and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, for example; personal contact details, video or images online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Do not be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as “friends” on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact pupils and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a pupil or parent/carer that may compromise this or have any queries or concerns about this, please speak to Designated Safeguarding Lead, Maddy Jones.

Documents called “Cyberbullying: Supporting School Staff”, “Cyberbullying: advice for headteachers and school staff” and “Safer professional practise with technology” are available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com, www.e-safety.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager, the Designated Safeguarding Lead, Maddy Jones or myself if you have any queries or concerns regarding this.




Please read through the attached Acceptable Use Policy, Sign and return **one** copy to the school office within two weeks of your start date.

Yours sincerely,
Mrs Abigail Birch, Executive Headteacher




Appendix 2

Ifield School Pupil Acceptable Use Policy




Ifield School Acceptable Use Poster




I only go online with an adult


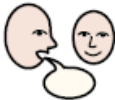



I am kind online




I keep information about myself safe





I tell an adult if something online makes me unhappy





Ifield Sixth Form Acceptable Use Poster







An adult knows what I do online







I keep information about myself safe

I tell an adult if something online makes me feel unhappy or unsafe

I share my online experiences with an adult

Appendix 4



Kings Farm School Staff Acceptable Use Policy 2017/18

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

20. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
21. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
22. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
23. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 6 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly every 60 days).
24. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
25. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN/DirectAccess). Any images or videos of pupils will only be used as stated in the school image use policy ([Link to image use policy](#)) and will always take into account parental consent.
26. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I

- will use staff drives to upload any work documents and files in a password protected environment via VPN/DirectAccess. I will protect the devices in my care from unapproved access or theft.
27. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
 28. I will respect copyright and intellectual property rights.
 29. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces, http://www.ifieldschool.com/cms/media/keyinfo/ifield_school_e-safety_policy_spring_2016.pdf
 30. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead, Chris Jackson as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Chris Jackson, Designated Safeguarding Lead and/or the designated lead for filtering Michael Sims as soon as possible.
 31. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Manager, Michael Sims as soon as possible.
 32. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.
 33. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.
 34. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
 35. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
 36. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead, Chris Jackson.
 37. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name:



Parents Acceptable Use Policy

- I have read and discussed the Acceptable Use Poster (attached) with my child where appropriate
- I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school Acceptable Use Policy then actions will be applied in line with the school's behaviour and anti-bullying policy and liaise with other agencies
- I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset or compromise the safety of any member of the school community
- I know that I can speak to the school Online Safety Coordinator, Maddy Jones, my child's teacher or the Executive Headteacher if I have any concerns about online safety
- I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org, www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- I will support the school and my child by role modelling and monitoring safe and positive online behaviour such as sharing images, text and video responsibly and by discussing online safety with them when they access technology at home.

I have read the Parent Acceptable Use Policy.

Child's Name..... Class.....

Parents Name.....Parents Signature.....

Date.....



Dear Parent/Carer,

All pupils use computer facilities including Internet access as an essential part of learning. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This includes access to: computers, laptops and other digital devices

- Internet which may include search engines and educational websites
- School learning platform/intranet
- Email
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphone's

The Cedar Federation recognises the essential and important contribution that technology plays in promoting pupil's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online safety (e-Safety) policies and procedures alongside the school's safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. However no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the schools internet and ICT facilities.

The Online safety Policy can be found on the school website under "Policies" or on request.

We request that all parents/carers support the schools approach to online safety (e-Safety) by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that pupils themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about online safety, we request that you read the attached Acceptable Use Policy with your child and that, where appropriate, you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school online safety co-ordinator, Maddy Jones or myself.

We understand that your child may be too young or have complex learning needs to be able to give informed consent on his/ her own; however, we feel it is good practice to involve them as much as possible in the decision making process, and believe a shared commitment is the most successful way to achieve this.

Please read through the attached Acceptable Use Policy, Sign and return to the school office.

Yours sincerely,

Mrs Abigail Birch, Executive Headteacher

Appendix 6

Safeguarding Incident Forms



SAFEGUARDING INCIDENT / CONCERN FORM

Pupil name:	DOB and Year Group:
Name and role of person completing form (please print):	
Date of incident /concern:	Time of incident/concern:
Incident/concern (Verbatim recording and who, what, where, when):	
Any other relevant information (witnesses, immediate action taken):	
Action taken:	
Signature of person completing form:	Date form completed (DD/MM/YY):
DSO or DSL action (including reasons and outcomes):	
Signature of DSO:	Date (DD/MM/YY):
Signature of DSL:	Date (DD/MM/YY):



King's Farm Primary School

Cedar Avenue
Gravesend
Kent DA12 5JT

Tel: 01474 566979

Fax: 01474 567767

Email: office@kings-farm.kent.sch.uk

Website: www.kings-farm.kent.sch.uk

Head of School: Mr Chris Jackson

SAFEGUARDING INCIDENT/CONCERN FORM

Pupil / Child Name:	DOB and Year Group / Class:
Name & Position of person completing form (please print)	
Date of incident / concern: (DD MM YY)	
Any other relevant information (Witnesses, immediate action taken)	
Signature: (Name of member of staff)	Date form completed (DD MM YY)
Role:	
Action Taken (Including reasons for decisions) and Outcomes* (NB – this section is only to be completed by DSL)	
Signature of DSL:	Date: (DD MM YY)
Signature of Lead DSL: (if appropriate)	Date: (DD MM YY)

*continue on a separate sheet if necessary

