Castleford Park Junior Academy

Online Safety Policy

Updated January 2022

Next Review Due January 2023

Aims and Rationale

This policy will be reviewed annually and in consultation with:

- Governors, Teaching Staff and Support Staff, students / pupils and parents

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body on:	*January 2021*
The implementation of this Online Safety policy will be monitored by the:	*Computing Coordinator and DSL as part of their safeguarding duties*
Monitoring will take place at regular intervals:	*Annually*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2022*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LADO, Police, SCD, CEOP*

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within CPJA:

The IT Service Provider Headteacher and computing leader will ensure:

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- that CPJA's technical infrastructure is secure and not open to misuse/malicious attack
- that CPJA meets required online safety technical requirements
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *internet* is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher, DSL or computing lead.
- that monitoring software / systems are updated as agreed in CPJA policies

- That harmful online challenges and hoaxes are managed following DFE guidance: https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes

The Head teacher and Deputy Designated Safeguarding Leads:

- Have a duty of care for ensuring the safety (including online safety) of members of the school community.
- All members of the above team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Co-ordinator.
- The Senior Leadership Team will receive updates from the School Council – via the School Council Lead – of any reported threats that children are experiencing outside of school – so that awareness can continue to be raised in school for other pupils and parents

The Headteacher/Deputy Designated Safeguarding Leads:

- Take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school online safety policies and additional documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provide training and advice for staff

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

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

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current CPJA Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement

- they report any suspected misuse or problem to the Senior Leadership Team for investigation
- all digital communications with students / pupils / parents / carers is on a professional level and only carried out using official school systems – as stated in the staff code of conduct and reviewed in regular 'Safer Working Practices' training
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

- are responsible for using CPJA's digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so -and how to keep themselves and others safe when online
- will be expected to know and understand policies on the use of mobile devices such as iPads and chrome books. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the CPJA's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. CPJA will take every opportunity to help parents understand these issues through parents' evenings, newsletters, websites, reference to guidance which will be shared on the school website and on learning platforms. Parents and carers will be encouraged to support CPJA in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices at home and when brought to school

Rationale

Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum where safety messages can be reinforced. Children are taught about internet safety through:

- Planned online safety lessons that are revisited at the beginning of each half term and through their PSHCE lessons

(Using the following guidance:
https://new.thinkuknow.co.uk/professionals/resources/
http://www.childnet.com/resources/esafety-and-computing/ks2

and using the resources provided from www.ticbradford.com

- Every year the school supports Safer Internet Day and online safety lessons are taught in this week using the guidance from https://www.saferinternet.org.uk/safer-internet-day/2021

- A planned programme of assemblies that reinforce safety and online vigilance
- Reminders in all lessons, where needed, to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Providing a safe environment for debate in order to support pupils in building resilience to radicalisation
- Being helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside CPJA.
- Staff acting as good role models in their use of digital technologies, the internet and mobile devices
- Ensuring that in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Vulnerable pupils – such as SEN, LAC or disadvantaged

Children with SEND are more likely than their peers to experience online issues, in particular: cyberbullying, online grooming and exploitation. Similarly, children with SEND are more likely to have their internet use restricted and therefore have limited opportunities to learn through experience, develop resilience or seek support, which would empower them to use technology safely. Online safety is therefore a fundamental part of our wider safeguarding responsibilities and education settings need to implement a range of targeted or differentiated online safety strategies in order to enable learners with SEND to access the internet safely and appropriately.

The school will do the following to support more vulnerable users:

- Build a collective terminology that all pupils understand. Staff will not assume that pupils have clear knowledge of what all vocabulary might mean – particularly abstract language
- Ensure that staff have a clear understanding of what individuals already know and understand before teaching more about online safety
- Differentiate accordingly, as in other subject areas, to suit the needs of the pupil(s)

- Allow pupils to use the real tools and practically explore what they are being taught (eg: https://www.thinkuknow.co.uk/professionals/resources/know-your-friends-with-josh-and-sue/)
- Demonstrate that breaking the rules has consequences, so that more vulnerable users understand the impact
- Educate all parents so that they are able to continue educating their children at home
- Work with the school SENCO and parents to ensure an individuals' needs are properly met
- Bear in mind that it might be easier for pupils who are trying to report an online concern to show the adults rather than having to tell them

Education & Training – Staff / Volunteers/Governors

All staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will take place as part of Safeguarding annual training
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the CPJA Online Safety Policy and Acceptable Use Agreement and as part of bi-annually reviewed Safer Working Practices training
- Participation in CPJA training for staff and parents (this may include attendance at assemblies)

Technical – infrastructure, filtering and monitoring:

The CPJA computing team (made up of a technical expert as part of an SLA and the computing staff team in school) will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audit of the safety and security of the CPJA technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users have clearly defined access rights to CPJA technical systems and devices.
- All users are provided with a username and secure password by the IT team at Castleford Academy
- The administrator passwords for the CPJA ICT system, used by the Network Manager must also be available to the Headteacher and Business Manager and kept in a secure place
- The Business Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, mobile devices from accidental or malicious attempts which might threaten the

security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data will not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety Education Programme.

- The school Acceptable Use Agreement for staff and the code of conduct, also gives consideration to the use of mobile technologies

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Written permission is also obtained to consent to school's use of 'Seesaw' and Google Classroom our secure, file-sharing platforms so that their children's work can be shared with them.

- Written permission is also obtained to consent to school's use of 'Bloomz'- a secure, file-sharing platform which celebrates pupil achievement both at home and at school.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at CPJA events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital or video images. The school obtains permission from parents of photographs to be taken of productions/special events in which children are due to appear in.
- Staff and volunteers are allowed to take digital / video images to support educational aims. Those images should only be taken on CPJA equipment, the personal equipment of staff should not be used for such purposes. These photos should stay on the school server and not be transferred between the place of work and home by any staff member
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or CPJA into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission - pupils who do this without consent will have follow up consequences involving their parents – see our anti-bullying policy for serious incidents such as cyber-bullying
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with a photograph of that pupil only.
- Pupil's work can only be published with the permission of the pupil and parents/ carers.
- Staff will role model acceptable use of photographs by asking pupils before taking any photos of them

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section in the appendix)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- Report any breaches or potential breaches to school – who will report this to the DPO (Designated Protection Officer)

When personal data is stored on any portable computer system, memory stick/hard drive or any other removable media:

- the data and device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Staff are encouraged to only use portable devices for storing data in an emergency or when most practical. All staff have access to a cloud-based filing system as part of their internet access and any temporarily stored data on portable devices should be transferred to this system as soon as possible.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render CPJA or

Castleford Multi-Academy Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

CPJA provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school in the following ways:

CPJA staff should ensure that:

- No reference is made in social media to pupils, parents / carers or CPJA staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Staff are not linked to parents/pupils or ex-pupils on any social media website
- Personal opinions can not be attributed to CPJA or the Multi-Academy Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official CPJA social media accounts are established there should be:

- A process for approval by senior leaders – staff must screenshot the comments that they would like to add and ask for approval – via email – from the Senior Leadership Team
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff (The Headteacher and Deputy Headteacher)

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others in the following way:

- Responding to the parent who made the post asking them to follow official complaints procedures where there is a problem reported
- Reporting the account to the relevant body (Facebook/Twitter etc)
- If a member of staff, or child is named; the parent will be contacted and will be given a specific amount of time to remove the post before it is referred to the relevant police department

Included Appendices:

1. **Pupil and parent online agreement**
2. **Staff and volunteer acceptable use agreement**
3. **Flow chart for reporting Online Incidents and securing evidence**
4. **The use of cameras and images within education settings policy**

Appendix 1

Pupil and Parent Acceptable Use Agreement

We request that parents discuss this acceptable use agreement thoroughly with their child(ren) as far as they are able to understand it, as the guidelines in it are ones that they will also need to abide by when moving to further education and into a job.

Academy Policy

Digital technologies have become very important to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe whilst using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put their personal security, or the security of the school and others within it, in danger.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people- helping them understand safe on-line behaviour.
- That CPJA will try to ensure that students will have good access to relevant computing technology to enhance their learning and will, in return, expect pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

1. **For my own personal safety:**

- I understand that CPJA will monitor how I use computers/iPad/chrome books, emails and other digital communications when I am on the school site.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details, family details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

- I understand that CPJA systems and devices are for educational use and that I will not use them for personal use unless I have permission to do so.
- I will not use CPJA systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (eg YouTube).

2. <u>I understand that everyone has equal rights to use technology as a resource:</u>

- I understand that CPJA computer systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

<u>3. I will act as I expect others to act toward me:</u>

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I respect the fact that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

<u>4. I recognise that the school has a responsibility to maintain the security of the technology it offers me and to ensure the smooth running of the school:</u>

- I will only use my personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any faults or damage to equipment or software, however this may have happened.

- I will not open any attachments to emails, without permission from a teacher, due to the risk of an attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

5.When using the internet for research or recreation, I recognise that:

- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I will take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

6. I understand that I am responsible for my actions, both in and out of school:

- I understand that CPJA also has the right to take action against me if I am involved in incidents of inappropriate behaviour that are covered in this agreement, when I am out of school. Particularly where it involves others from the school community (examples would be cyber-bullying, use of images or personal information).
- If I do not follow the rules for using the computers, there may be a consequence which could involve not being able to use them in the future.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the *pupil* Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use CPJA systems and devices (both in and out of school)
- I use my own devices in academy grounds (when allowed) e.g. mobile phones, gaming devices USB devices, cameras, iPads, chrome books etc.
- I use my own equipment out of the academy in a way that is related to me being a member of CPJA e.g. communicating with other members of the school, accessing school email, accessing Google classroom, website or platforms such as Bloomz or Seesaw.

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Parent / Carer Countersignature .....

Name of Parent/Carer: .....

Appendix 2

Staff (and Volunteer) Acceptable Use Agreement

CPJA Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and develop awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people – through teaching and through being an effective role model for online safety myself.

For my professional and personal safety:

- I understand CPJA will monitor my use of the school digital technology and communications systems that I use.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, platforms such as Bloomz, Seesaw etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational where permission has been granted.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone will steal it.
- I will not leave a computer/iPad logged in with my username if it is then left unsupervised.
- I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person within school.

I will be professional in my communications and actions when using *academy* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take, or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (e.g. on the school website / learning platform) it will not be possible to identify by name, or other personal information, those who are featured.

I will be professional in my communications and actions when using *my own social media outside of the school setting.*

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- When using social networking sites and other services for personal use I will not say anything that could bring CPJA , staff members or any member of the school community into disrepute.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will ensure that I do not refer to students, pupils, parents/carers or school staff on social media.
- I will not engage in any online discussion about the school or any members of the school community unless this is in an approved context e.g. school own Twitter account
- I will not attribute my personal opinions to CPJA on social media and will make clear that they are my own opinions
- I will immediately report any online discussion that could impact on CPJA / staff reputation and any negative postings about any member of our school community
- I will not have parents/pupils or ex pupils as 'friends' on any social media websites or similar systems.
- I will inform the appropriate member of staff in school if a parent/pupil/ex pupil tries to make contact with myself through social media.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *academy*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using CPJA equipment. I will also follow any additional rules set by CPJA about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on CPJA ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to CPJA equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or CPJA policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I understand that I must promote safe use of ICT systems to pupils at our academy:

- I will model safe use of technologies and the internet in school.
- I will educate young people on how to use technologies safely according to the school's e-safety teaching programme.
- I will take immediate action in line with CPJA policy if an issue arises in or out of school that might compromise learner, user or school safety; or if a child reports any concerns.
- I will monitor learner behaviour online when using technology and deal with any issues that arise.
- If I believe, a young person may be at risk I will follow the child protection procedures held by CPJA.
- If I believe a young person may be being bullied via technologies, I will follow the anti-bullying procedures laid out in the anti-bullying policy.

I understand that I must keep school data protected in line with Data Protection Act:

- When I use computer equipment at home, I will ensure resources cannot be accessed or copied by anyone else and that no one else uses the laptop.
- I will ensure personal equipment used is password protected.
- I will ensure that my data is regularly backed up.
- I will take all steps within my power to keep personal data safe and minimise the risk of losing it.
- I will only use personal data on secure devices that are password protected.
- When transferring data I will use encryption and secure password-protected devices.
- I will ensure that devices I use have approved virus and malware checking software and I will delete data securely once it has been transferred or finished with.
- I understand that data protection requires that any personal data that I have access to must be kept private and confidential, except when I am required by law or by school policy to disclose it to an appropriate authority.

I understand that I am responsible for my actions in and out of CPJA :

- I understand that this Acceptable Use Policy applies not only to my work and use of CPJA digital technology equipment in school, but also applies to my use of academy systems and

equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Trustees and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

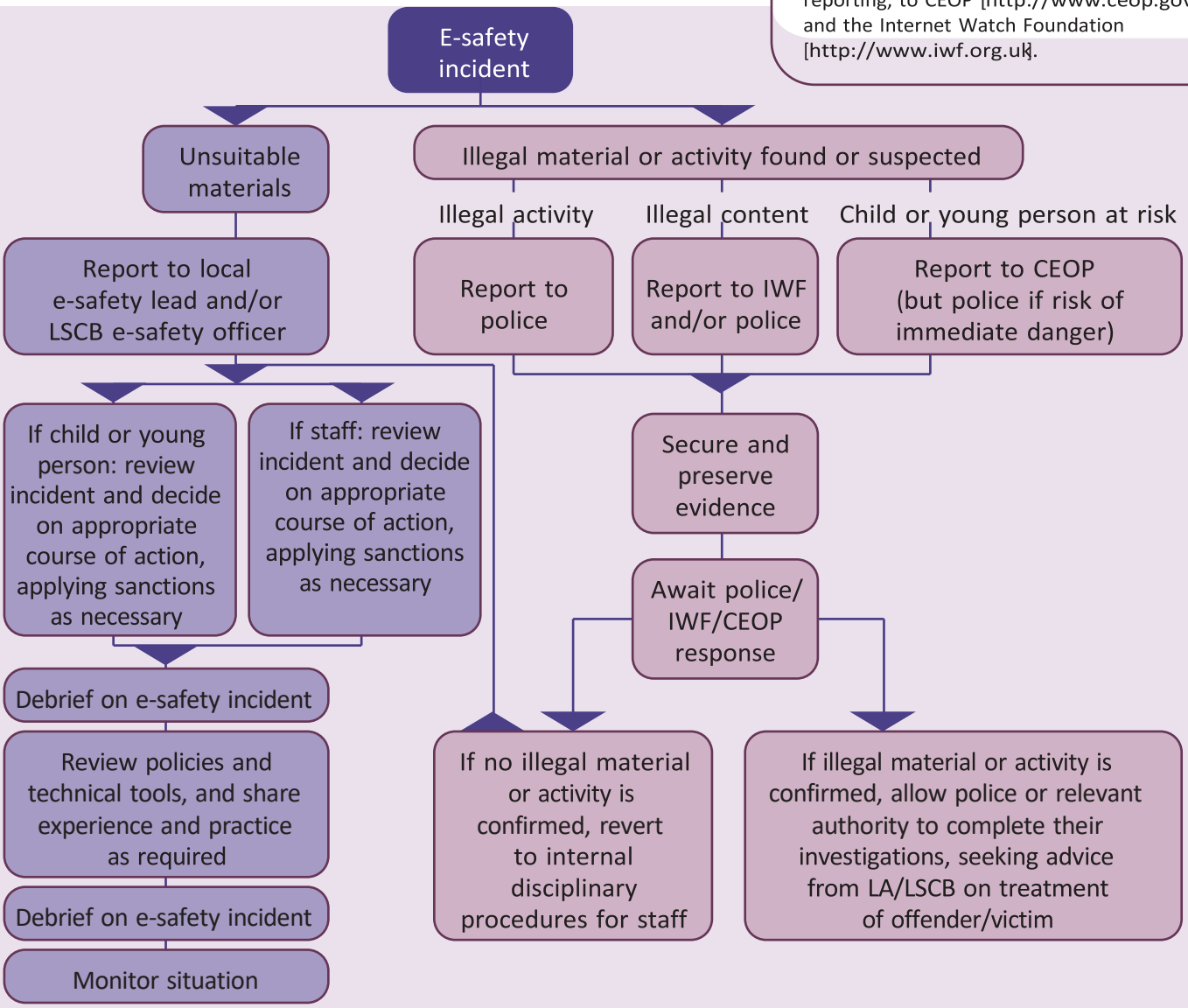
Signed: .....

Date: .....

Appendix 3

Flowchart for responding to e-safety incidents and securing evidence

Note: this flowchart originally appeared as 'Flowchart for responding to internet safety incidents in school' in the Becta publication *E-safety: Developing whole-school policies to support effective practice*. We have revised and updated it to include additional lines of reporting, to CEOP [http://www.ceop.gov.uk] and the Internet Watch Foundation [http://www.iwf.org.uk].



Appendix 4

CASTLEFORD
PARK JUNIOR ACADEMY

The Use of Cameras and Images Policy

Updated January 2022

Date of next review: January 2023

The Use of Cameras and Images Policy

Rationale

- All images taken by the Academy will be used in a manner respectful of the eight Data Protection Principles. This means the images will be:
- Fairly and lawfully processed
- Processed for limited, specifically stated purposes only
- Used in a way that is adequate, relevant and not excessive
- Accurate and up to date
- Kept on file for no longer than is necessary
- Processed in line with individual's legal rights
- Kept securely
- Adequately protected if transferred to other countries

Guidelines for Acceptable Use:

- Written consent must be obtained from parents before photographs are published – a record of consent will be securely kept on file. If a parent chooses to withdraw consent, images already on file will be destroyed.
- Written consent must also be obtained from any adults who may have photographs published
- Personal details (such as first name and surname) should not be used alongside images (A drawn image could be an acceptable way to avoid this)
- Where group, or class photographs are used, their accompanying text should be general (e.g. 'Making Christmas Decorations' or 'An Exciting Science Lesson!')
- Images will not be taken against a child's wishes and photography is not permitted in sensitive areas such as changing rooms, toilets, swimming areas etc.
- Photos of pupils, or adults who have left the school cannot be used.
- It is important that permission is sought for online use of photos as well as use of photos in school
- Staff should use school property to take all photos, or videos of children and should be downloaded onto the school system for use – all images remain onsite at all times.
- Any images that need to be transported must be encrypted – including those to be sent by e mail.
- An E-safety risk assessment will be carried out for any online platforms or websites that school is considering using to ensure that it complies with the Data Protection Act.
- Parents are allowed to take pictures, or recordings of their own children for their personal use but they must be made aware of this and the consequences of selling or distributing such images without proper permission. Parents will fill in a form to agree not to share these images on social media.
- Staff will ensure that any devices they use whilst in school and that are entrusted into their possession are secure –and only accessibly by them – at all times. They are also locked away securely when not in use in case of theft

- Professional photographers engaged to work with the school will agree to work under the school's online safety policy settings and in accordance with the Data Protection Act of 1998 – they will be asked to sign this policy documenting this.
- All areas covered with CCTV will be well signposted so that individuals are advised before entering the vicinity and are appropriately placed. Recordings are disposed of after 30 days.
- When children are using digital cameras or videos:
- They will be appropriately supervised throughout.
- All images and videos taken are monitored by the teacher and stored on a school device
- Appropriate and acceptable use will be discussed with them.
- Parents will be informed that this is the case and permission will be sought before this happens.

Online Safety Policy Monitoring and Review:

This policy will be reviewed annually and approved by the following people:

Head teacher: K. Law

Business Manager: K. Ineson

Online Safety Co-ordinator: L Sanpher

IT Services: J. Randall and M. Robinson

Chair of the Governing Body: T. Sycamore

Date of next Review: January 2023

Signed  Date: Jan 2022

Miss K. Law Headteacher

Signed  Date: Jan 2022

Mrs T. Sycamore Chair of Governors

Signed Date: Jan 2022

Mrs L. Sanpher Online Safety Co-ordinator