Castleford Park Junior Academy Online Safety Policy

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 Board of Directors / Governing Body / Governors Sub Committee on:	*Sept 2017*
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:	*September each year*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LADO, Police, SCD*

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 / academy ICT systems, both in and out of the *academy*.

Roles and Responsibilities

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

The IT Service Provider (Castleford Academy) will ensure:

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

- 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*
- *that monitoring software / systems are implemented and updated as agreed in school / academy policies*

The Head teacher/Designated Senior Lead:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be 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 / Senior Management Team will receive regular monitoring reports from the Online Safety Co-ordinator / Officer.

The Designated Safeguarding Lead/Computing Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- reports regularly to Senior Leadership Team

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 academy 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 *Headteacher* for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy and acceptable use policies
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students / Pupils:

- are responsible for using the *school / academy* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *academy'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 / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, website / literature. Parents and carers will be encouraged to support the academy 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 where this is allowed

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 once a term

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

- 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 student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.
- 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.

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 academy Online Safety Policy and Acceptable Use Agreements.
- Participation in academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure, filtering and monitoring:

The academy computing team 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 audits of the safety and security of the academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by the IT team at Castleford Academy
- The administrator passwords for the academy ICT system, used by the Network Manager (or other person) 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, work stations, mobile devices etc 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 Agreements for staff, give 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 students / 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 students / 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 students / pupils are published on the school website / social media / local press
- Written permission is also obtained to consent to school's use of 'Seesaw' a secure, file-sharing platform so that their children's work can be shared with them
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy 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 / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims. Those images should only be taken on school / academy 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 students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' / Pupils' full names, or even first names will not be used anywhere on a website or blog, particularly in association with a photograph of that pupil only.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or 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 academy 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.

When personal data is stored on any portable computer system, memory stick 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

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 the academy or academy group liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

School / academy staff should ensure that:

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

When official school / academy 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
- The account will be reported to the appropriate 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

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

Head teacher: K. Law

Business Manager: C. Probert

IT Services: J. Randall

Member of the Governing Body: S. Churm

Date of next Review: September 2018

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**