JERRY CLAY ACADEMY

E-SAFETY POLICY

This policy was last reviewed on	July 2022
This policy is scheduled for review on	July 2024

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the Trustee Board

Monitoring of the E-Safety Policy will take place at regular intervals.

The Governing Body will receive a report on the implementation of the E-Safety Policy.

The E-Safety Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be September 2024.

The Academy will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of:
  - students
  - parents/carers
  - staff

Scope of the Policy

This policy applies to all members of Jerry Clay Academy (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Jerry Clay Academy ICT systems, both in and out of Jerry Clay Academy.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber- bullying, or other e-safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Jerry Clay Academy will deal with such incidents within this policy and associated behaviour and anti- bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of Academy.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Jerry Clay Academy.

GOVERNORS:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about e-safety incidents and monitoring reports. The Safeguarding trustee will oversee E-Safety. The E Safety role will include:

- regular meetings with the Headteacher
- regular monitoring of e-safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

HEADTEACHER AND SENIOR LEADERS:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the Academy community, though the day to day responsibility for e-safety will be shared by member of the Senior Leadership Team and Computing Subject Leader.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse").
- The Headteacher/Senior Leadership Team are responsible for ensuring that the ICT Leader and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in the Academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Leader.

E-SAFETY COORDINATOR/DESIGNATED SENIOR PERSON (HEADTEACHER)

- leads on e-safety issues
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the relevant body
- liaises with Primary ICT support
- receives reports of e-safety incidents and creates a log of incidents to inform future e- safety developments

- meets regularly with E-Safety Governor (Safeguarding Trustee) to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

NETWORK MANAGER (PRIMARY ICT SUPPORT):

The Network Manager is responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the Academy meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/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 e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/ E-Safety Coordinator/Designated Senior Leader for investigation/action/sanction.
- that monitoring software/systems are implemented and updated as agreed in Academy policies.

TEACHING AND SUPPORT STAFF:

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current Academy e-safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Agreement .
- they report any suspected misuse or problem to the Headteacher/E-Safety Coordinator/Designated Senior Person for investigation/action/sanction.
- all digital communications with students/parents/carers should be on a professional level and only carried out using official Academy systems.
- e-safety issues are embedded in all aspects of the curriculum and other activities.
- students understand and follow the e-safety and acceptable use agreements.
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned students 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

CHILD PROTECTION/SAFEGUARDING DESIGNATED LEAD (HEADTEACHER)

The Child Protection/Safeguarding Designated Person should be trained in e-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

PUPILS:

- are responsible for using the Academy digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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 e-safety practice when using digital technologies out of Academy and realise that the Academy's E-Safety Policy covers their actions out of Academy, if related to their membership of the Academy.

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, letters, website and information about national/local e-safety campaigns/literature. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events.
- access to parents' sections of the website and on-line student records.
- their children's personal devices in the Academy (where this is allowed)

Policy Statements

EDUCATION – STUDENTS

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Academy's e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum provided as part of ICT/PHSE/other lessons and is regularly revisited.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and day to day pastoral activities in class.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Academy
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

EDUCATION – PARENTS/CARERS:

Parents/carers play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (see appendix for further links/resources)

Education – The Wider Community:

The school/academy will provide opportunities for local community groups/members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school/academy website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision.

EDUCATION & TRAINING – STAFF/VOLUNTEERS:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-safety policy and Acceptable Use Agreements.
- The E-Safety Coordinator/Designated Senior Person (or other nominated person) will receive regular updates through attendance at external training events/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

TRAINING – TRUSTEES:

Trustees should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/e-safety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation.
- Participation in Academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

REMOTE LEARNING

As a school, we use Microsoft teams for online remote meetings and learning. The staff agreement below sets out our expectations when using this. All children in school are part of a class on teams. Children have also had training for using teams safely and this has been included on their agreement also. The use of the remote learning has seen our pupils upskilling their ICT skills which prepares them for life in the modern age

Remote learning protocol (Microsoft Teams)

- When delivering remote education online the same principles set out in the staff Code of Conduct will apply.

- Staff should have in mind their safeguarding obligations and should report any safeguarding concerns according to the school policy.

- All staff should wear appropriate clothing, the background should be neutral and desk/ table should be clear.

- Other household members should not be seen on the screen, and whilst online you should not be interrupted.

- Microphones should be muted when the input is finished so that incidental conversations cannot be heard.

- An indication of how long the session will be and when the children should sign in and out needs to be sent to the children vial a weekly timetable. If bubble closure doesn't allow for this, do this as soon as possible

- Staff can move away from the computer once lesson input has been given to allow children to work independently. If this is done, ensure that you click the red leave button, then end meeting.

- Staff should remain professional at all times.

- Make sure that any other tabs that are open in the browser are appropriate for a child to see if you are sharing a screen.

- Decide if you are going to disable chat as this can be a distraction to learning.

- Always use 'End Meeting' on the red button to ensure that no children remain on TEAMs unsupervised.

- Always take a register for each session and record any incidents or issues as well as informing SLT.

- Use teams to schedule meetings and ensure that you don't allow others to bypass the lobby. This means that the session cannot start without you.

The children should be taught the following to enable the sessions to run smoothly:

- How to mute and use the hand symbol. The expectation is that they are on mute, unless told otherwise. How to turn their camera off, if required.
- They should be dressed appropriately and have the resources they need to hand.
- The children should be in a quiet place, free from interruptions with an appropriate background behind them. This space should be a shared space in their house.
- Classroom standard of behaviour is expected from all participants.

TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING:

The Academy will be responsible for ensuring that the Academy infrastructure/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 e-safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of Academy technical systems
- All users will have clearly defined access rights to Academy systems and devices.
- All users will be provided at KS2 and above with a username and secure password. Users are responsible for the security of their username and password.

- The “master/administrator” passwords for the school/academy systems, used by the Network Manager (or other person) must also be available to the *Headteacher* when required and Primary ICT provide technical support where needed to follow up any inappropriate use of the academy systems.
- Primary ICTis 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. CPOMs software licensing is dealt with by the business manager.
- The Academy has provided enhanced/differentiated user-level filtering
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Filtering changes can be requested by contacting the service desk via email: support@primaryictsupport.co.uk
- Primary ICT Support regularly monitor and record the activity of users via the Securly Web Filtering system on the Academy systems and users are made aware of this in the Acceptable Use Agreement. Member of the Designated Safeguarding Team are informed of any blocked or flagged activity.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. Office 365 automatically monitors any breaches and accounts are protected with two factor authentication.
- 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 devices are protected by up to date virus software. - A Barracuda Firewall has been provided to protect the network perimeter, the Server and all devices are proactively maintained and updated to ensure maximum security. All passwords have been configured in line with the Government’s Cyber Essentials recommendation. All devices, where possible, have Avast Anti-Virus Professional Plus deployed.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the Academy systems.
- An agreed policy is in place regarding the extent of personal use that users are allowed on Academy devices that may be used out of Academy.
- Users are not permitted to download and or install applications (including executable or similar types) on to an Academy device or whilst using the Academy’s systems, without agreement from the IT department.
- *An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.* See Appendix 1

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be provided by Jerry Clay Academy 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.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, staff conde of conduct, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- **The Jerry Clay Academy acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No[1]*	*Yes[2]*	*Yes/No**Error! Bookmark not defined.***

Personal devices:

- *[1]Older pupils (normally Year 6) may bring mobile phones to school if parents/carers wish them to have them if making their own way to and from school. These are stored securely in the school office and not available to the pupils during the school day.*
- *[2]Condition relating to staff using personal devices are set out in the Code of Conduct:*
- Whilst staff are using personal devices for work purposes, including accessing WiFi whilst on school premises then the standards set out in the Code of Conduct apply.
- The personal use of mobile phones during working hours should be undertaken with discretion and primarily restricted to dealing with emergencies. Staff should not make or receive calls of texts or use social media during work time where pupils are present. Mobile phones should be on silent at all times whilst in school and should not be left on display, with the exception of the staff room.
- Staff are not permitted to use their personal devices for making voice of video recordings within school or taking photos of pupils. If there is a requirement in the individual's role to take photographs of children for school purposes, this should be carried out using school equipment which will be provided with the agreement of the Headteacher and in line with the agreed schools procedures and where appropriate permissions have been sought.
- No technical support is available for personal devices in the academy.
- Jerry Clay Academy reserves the right to take, examine and search users devices in the case of misuse– This is also included in the Academy Behaviour Policy.
- School accepts no liability for loss/damage or malfunction following access to the network
- Visitors will be informed about school requirements by the welcoming office staff.
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

USE OF DIGITAL AND VIDEO IMAGES:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 Academy 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 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.
- 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 is 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 students in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website.
- Student's work can only be published with the permission of the student and parents or carers.
- Staff use two factor authentication to access files when on and off site.

DATA PROTECTION:

Jerry Clay Academy must ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).

- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. Jerry Clay Academy has a clear 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Jerry Clay Academy has systems in place to identify inaccuracies, such as asking parents to check emergency contact details at the start of each academic year.
- it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice.
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- Data Protection Impact Assessments (DPIA) are carried out. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- it has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)

- device must be protected by up-to-date virus and malware checking software
- data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any academy personal data to personal devices except as in line with school policy
- access personal data sources and records 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

COMMUNICATIONS:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff & other adults			Students/Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school/academy	X						X y5/6	
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X

Taking photos on mobile phones/cameras		X						X
Use of other mobile devices e.g. tablets, gaming devices	X							X
Use of personal email addresses in school/academy, or on school/academy network				X				X
Use of school/academy email for personal emails				X				X
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs	X					X		

When using communication technologies, the school/academy considers the following as good practice:

- **The official school/academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and students/pupils should therefore use only the school/academy email service to communicate with others when in school, or on school/academy systems (e.g. school Office 365 account).
- **Users must immediately report, to the headteacher– in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) academy systems including ParentMail and Seesaw. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above may be provided with individual school/academy email addresses for educational use
- Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school/academy website and only official email addresses should be used to identify members of staff.

SOCIAL MEDIA - PROTECTING PROFESSIONAL IDENTITY:

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school/academy and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school/academy protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *academy* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Jerry Clay Academy staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *academy*
- 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*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Jerry Clay Academy permits reasonable and appropriate access to private social media sites

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 according to a defined policy or process
- Jerry Clay Academy's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the school policies

APPROPRIATE AND INAPPROPRIATE USE BY STAFF OR ADULTS:

Staff members have access to the network so that they can obtain age-appropriate resources fortheir classes and create folders for saving and managing resources.

They have a password to access a filtered internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff should receive a copy of the E-Safety Policy and a copy of the Acceptable Use Agreement, which they need to sign, return to the Academy, to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Agreement will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

IN THE EVENT OF INAPPROPRIATE USE

If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the Headteacher/Senior Designated Person immediately and then the Managing Allegations Procedure and the Safeguarding and Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

APPROPRIATE AND INAPPROPRIATE USE BY CHILDREN OR YOUNG PEOPLE:

Acceptable Use Agreements detail how children and young people are expected to use the internet and other technologies within Academy, including downloading or printing of any materials. The agreements are there for children and young people to understand what is expected of their behaviour and attitude when using the internet. This will enable them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child, or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The Academy should encourage parents/carers to support the agreement with their child or young person. This can be shown by signing the Acceptable Use Agreements together so that it is clear to the Academy/education setting or other establishment that the agreement are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond Academy/education setting or other establishment.

Further to this, it is hoped that parents/carers will add to future rule amendments or updates toensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means online should be appropriate and be copyright free when using the learning platform in or beyond Academy/education setting or other establishment.

Dealing with unsuitable/inappropriate activities

Should a child or young person be found to misuse the online facilities whilst at Academy, the following consequences should occur:

- The parents /carers of any child found to be misusing the internet by not following the Acceptable Use Agreement will be contacted explaining the reason for suspending the child or young person's use for a particular lesson or activity.

- Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time.

- A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing online technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this may have legal implications.

Peer on peer abuse

Peer on Peer/Child on Child Abuse – sharing nudes & semi nudes/bullying/racism/sexual assaults/physical assault/hazing or initiating

Child on child abuse, will always be taken seriously and swiftly acted upon, under the appropriate policy e.g. safeguarding, behaviour, bullying and a risk assessment completed as required. Students will be encouraged to report any concerns freely.

It will not dismissed as 'banter' or 'part of growing up'. These issues will be part of PSHE /RSE lessons and discussions. Victims will be supported through the school's pastoral system.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Jerry Clay Academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy context, either because of the age of the users or the nature of those activities.

Jerry Clay Academy believes that the activities referred to in the following section would be inappropriate in an academy context and that users, as defined below, should not engage in these activities in/or outside the academy when using academy equipment or systems. Jerry Clay Academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	

	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism					X
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B Jerry Clay Academy will decide on a case by case basis whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways.						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)			X			
On-line gambling					X	
On-line shopping/commerce			X			
File sharing			X			
Use of social media		X				

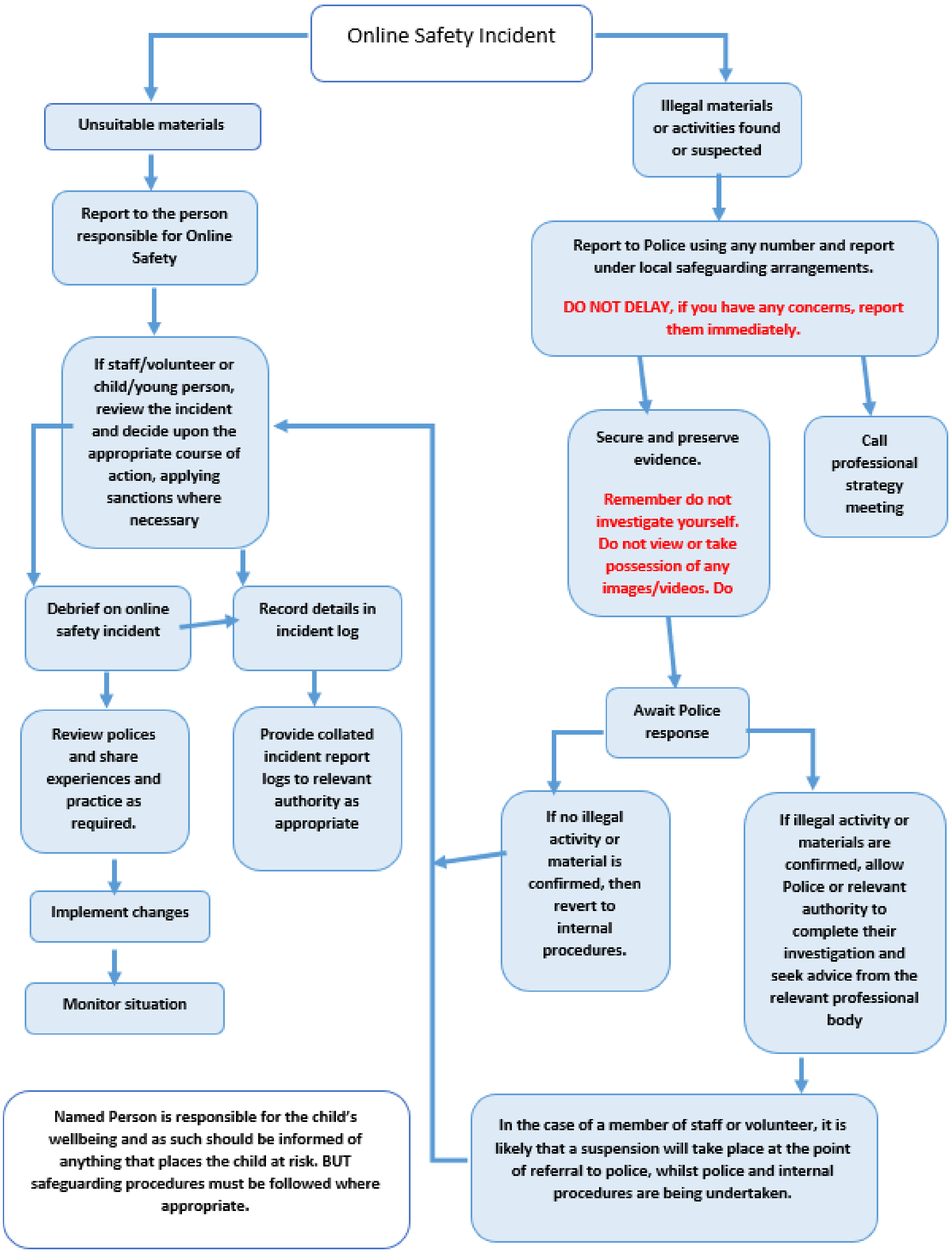
Use of messaging apps	X				
Use of video broadcasting e.g. Youtube	X				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the Jerry Clay Academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
    - Police involvement and/or action

- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *academy* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Jerry Clay Academy actions & sanctions -

It is more likely that Jerry Clay Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: - by referral to class teacher and Headteacher.

In the case of unauthorised or inappropriate use of the internet including mobile devices by children, parents will be informed. The Academy will employ a restorative approach to inform the child how the uses were inappropriate. Sanctions may be used if there is further inappropriate use following the normal behaviour and anti-bullying policies. This could include loss of access to the school network/internet, warnings or exclusions, contact with parents and in the event of illegal activities involvement of the police.In the case of illegal use of the internet, the police will be informed.

In appropriate use of the internet by staff should be reported to the Headteacher and Chair or Trustees. Where the actions violate the Staff Acceptable Use Agreement, the Staff Code of Conduct and Safeguarding Policy, additional action may be applied. Where actions are illegal, the Police will be informed.

APPENDIX 1

SECURE TRANSFER OF DATA AND ACCESS OUT OF ACADEMY

Jerry Clay Academy recognises that personal data may be accessed by users out of the Academy, or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the Academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of Academy
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should use two factor security to access devises and information.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe.

APPENDIX 2

JERRY CLAY ACADEMY

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer)

2022-23

Jerry Clay Academy 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 stimulate 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 while using the internet and other communications technologies for educational, personal and recreational use.
- that Jerry Clay 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.

Jerry Clay Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

This policy applies to any device in the Academy. It applies across the whole network and includes Wi-Fi.

Jerry Clay Academy carries out secure content inspection (SSL inspection). This means that when you access a site that uses techniques to secure the information between the website and yourself, Jerry Clay Academy can read the information and remove inappropriate content or prevent access to the material. Excluded from this inspection are sites that contain sensitive financial information, including banks and payment systems.

Your activity on the internet is closely monitored by the Academy, logs are kept of activity, whether on an Academy device or using your own device through the Academy Wi-Fi. These logs include who is accessing what material for how long from which device.

The Academy email system is provided for educational purposes, where required the Academy has the ability to access your Academy email for safeguarding purposes.

Acceptable Use Policy Agreement

I understand that I must use Jerry Clay Academy 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 and will ensure that students/pupils receive opportunities to gain from the use of digital technology. 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.

For my professional and personal safety:

- I understand that Jerry Clay Academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to Jerry Clay Academy ICT systems (e.g. laptops, email, etc.) out of Academy, and to the transfer of personal data (digital or paper based) out of Academy.
- I understand that Jerry Clay Academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Academy.
- 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 may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Jerry Clay Academy 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 and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- 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.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Jerry Clay Academy:

- When I use my mobile devices (PDAs/laptops/mobile phones/USB devices etc.) in Academy, I will follow the rules set out in this agreement, in the same way as if I was using Academy equipment. I will also follow any additional rules set by the Academy 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 the Academy 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 ensure that my data is regularly backed up, in accordance with relevant Academy policies.
- 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 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 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 Academy 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 E-Safety Policy, Appendix 3. 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 student 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 by Academy 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.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school/academy*:

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/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 school/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority 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: ---

ACCEPTABLE USE AGREEMENT

(Staff/Volunteer) 2022-23

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

Staff/Volunteer Name

Signed

Date

Please detach this page and return to the box in the Staff Room by *insert date*

APPENDIX 3

JERRY CLAY ACADEMY

Pupil Acceptable Use Agreement for KS2 pupils

2022-23

Pupil Acceptable Use Agreement for KS2 pupils

(E-Safety)

2022-23

Pupil Agreement

Digital technologies are an important part of our lives and we can use them to open up new opportunities for everyone. They can lead to interesting discussions, help me to be creative and help me to learn effectively. Young people have the right to safe access to these digital technologies.

I understand that I must only use the school's equipment in a responsible way to help keep everyone safe and happy when learning online.

LEARNING SAFELY

- I will only use the laptops and devices in school for school purposes.
- I will not tell other people my passwords.
- When I am using the internet to find information, I should take care to check the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I will not try to upload, download or access any materials that are illegal or inappropriate or may upset other people. I understand that the school internet is filtered to prevent access to such material.

RESPECT

- I will act as I expect others to act towards me.
- I will respect other's work and property and will not access, copy, remove or alter any other user's files without their knowledge and permission.
- I will be polite and responsible when I communicate with others. I appreciate that others may have different opinions.
- I will not deliberately look for, save or send anything that could offend or upset others.
- I will respect the school's systems by reporting any damage or fault no matter how it was caused.

ONLINE SAFETY

- I will not give out my personal details such as my name, phone number, home address, email addresses, age, gender or school.
- I will not disclose or share personal information about or images of other people when online.
- I will not take or distribute images of anyone without their permission.
- I will be responsible for my behaviour when using computers and mobile devices in school or at home because I know that these rules are to keep me safe.
- I will not normally arrange to meet someone off-line that I have communicated with online. If I do, I will ask an adult, do so in a public place and take an adult with me.
- I will not give anyone I communicate with online information about me or share photographs. I will tell a trusted adult if I am contacted by someone I don't know.
- I will only use my own school email address (if I have one) when emailing.
- I will only open hyperlinks or email attachments from people I know, or who my teacher has approved.
- If I accidentally find anything inappropriate on the internet, **I will tell my teacher or a trusted adult immediately.**
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online by telling my teacher or a trusted adult.
- I know that my use of computers can be checked and that my parent or carer contacted if a member of school staff is concerned about my safety.
- I will not use my own personal devices (mobile phones / USB devices / smart watches etc) in school unless I have permission.

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

I understand that Jerry Clay Academy has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are included in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online bullying or the use of images or personal information.)

I understand that if I fail to comply with this acceptable use agreement, consequences may be applied. This could include loss of access to the school network / internet, warning, contact with parents or in the event of illegal activities involvement of the police.

Children's Remote Learning Agreement. (Microsoft Teams)

When I am working on a computer in school or at home on a Microsoft Teams lesson:

1. I need to sit in a shared space in my house, where a parent/ carer is available if needed. This space should be quiet and free from interruptions.

2. I need to be dressed appropriately and I should have everything I need for the lesson ready, e.g. paper, pens, work booklet.

3. I will behave appropriately, as I would if I was in the classroom at school.

4. My teacher will tell me how to use the hand tool and I will use this sensibly if I need to.

5. I will mute my microphone if told, and leave it muted unless told otherwise.

6. I will not record the session.

7. My teacher will tell me how long the session will last and give me instructions about what to do. I will follow these carefully.

Name of Student/Pupil: ....

Group/Class: ....

Signed: ....

Date: ....

Pupil Acceptable Use Agreement for EYFS and KS1

2022-23

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet.

Parent/Carer Acceptable Use Agreement Template

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

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students/pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users. A copy of the *student/pupil* acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work

Permission Form

Parent/Carers Name: ....

Student/Pupil Name: ....

As the parent/carer of the above *students/pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or 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.

Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or 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 understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: ……………………………………………………………

Date: ……………………………………………………………

Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: ....
Date: ....
Reason for investigation: ....

....

....

Details of first reviewing person

Name: ....
Position: ....
Signature: ....

Details of second reviewing person

Name: ....
Position: ....
Signature: ....

Name and location of computer used for review (for web sites)

....

....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken
