Astrea Academy Trust

INSPIRING BEYOND MEASURE

Online Safety Policy

Date	September 2024
Written by	On Line Lead
Adopted by Trust Board	
Adopted by LGB	
Review Date	September 2025

LOWER MEADOW PRIMARY ACADEMY
Astrea Academy Trust
INSPIRING BEYOND MEASURE

Contents

1. Aims

Lower Meadow Primary Academy aims to provide the necessary safeguards to help ensure that all reasonable actions have been taken to manage and reduce the risks associated with communication technology and internet usage. This policy has taken into account the procedures and practice of the Local Safeguarding Children Board and Keeping Children Safe in Education 2023. This policy should be used alongside the Trust-wide Child Protection and Safeguarding Policy and the Academy's Preventing Extremism and Radicalisation Policy. The following policy outlines the measures that will be taken to reduce the risks, as well as addressing wider educational issues in order to help young people, their parents and staff to become responsible users and stay safe while using the internet and other communications technologies for educational or personal use.

- This policy applies to all members of the academy community including staff, pupils, parents/carers, volunteers and work placements, which have access to and are users of academy ICT (Information and Communication Technologies) systems both in and out of the academy.
- The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of the academy, but is linked to membership of the academy.
- The Education Act 2011 gives the academy the power to confiscate the contents of any mobile device if the Principal believes it contains any illegal content or material that could be used to bully or harass others
- The academy will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of the academy.

2. Communication of the Policy

Lower Meadow Primary Academy senior leadership team will be responsible for ensuring all members of academy staff and pupils are aware of the existence and contents of the academy online safety policy and the use of any new technology within the academy.

· The online safety policy will be provided to and discussed with all members of staff formally.
· All amendments will be published on the academy website and shared with staff during staff meetings.
· An online safety or online safety module will be included in the PSHE, Citizenship and/or ICT curricula covering and detailing amendments to the online safety policy.

· All new members of staff will be introduced to the online safety policy.
· Lower Meadow Primary Academy will hold an annual review of the online safety policy.
· Pertinent points from the academy online safety policy will be reinforced across the curriculum and across all subject areas when using ICT equipment within the academy.
· The key messages contained within the online safety policy will be reflected and consistent within all acceptable use policies in place within the academy.
· We endeavour to embed online safety messages across the curriculum whenever the internet or related technologies are used
· The key relevant online safety policy messages will be shared with all pupils during the academy year.

3. Roles and Responsibilities

3.1. The Principal has overall responsibility for online safety of all members of the academy community. Day to day responsibility will be delegated to the online safety co-ordinator. The principal will ensure that the online safety lead has access to relevant training to enable them to carry out their role and train other staff as necessary. The principal and senior leadership team will make themselves aware of the procedures to follow in the event of a serious online safety incident. The online safety lead is: **Amy Marshall**

3.2. The online safety lead will ensure:

- The academy online safety policy is current and pertinent
- The academy online safety policy is reviewed at regular intervals
- The academy acceptable use policies are appropriate for their intended audience.

Responsibilities of the online safety lead

- To promote safe internet and technologies use within the academy.
- To promote an awareness and commitment to online safety throughout the academy.
- To be the first point of contact in the academy on all online safety matters.
- To take day-to-day responsibility for online safety within the academy and to have a leading role in establishing and reviewing the academy online safety policies and procedures.
- To lead the academy online safety team
- To have regular contact with other online safety teams, e.g. Safeguarding Children Board
- To communicate regularly with computing technical staff working with the academy.
- To communicate regularly with the designated online safety governor.
- To communicate regularly with the senior leadership team.
- To create and maintain online safety policies and procedures.
- To develop an understanding of current online safety issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in online safety issues.

- To ensure that online safety education is embedded across the curriculum.
- To ensure that online safety is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children's Board and other recommended relevant agencies, as appropriate.
- To monitor and report on online safety issues to the online safety group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- To ensure that an online safety incident log is kept up to date.
-

3.3 Teachers and support staff will be responsible for the following actions:

- To read, understand and help promote the academy's online safety policies and guidance.
- To read, understand and adhere to the academy staff Acceptable Use Policy.
- To report any suspected misuse or problem to the online safety coordinator.
- To develop and maintain an awareness of current online safety issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through academy based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones etc.
- To embed online safety messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of online safety issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the academy.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using encrypted data storage and by transferring data through secure communication systems.

3.4 Technical Support Staff will be responsible for the following actions:

- To read, understand, contribute to and help promote the academy's online safety policies and guidance.
- To read, understand and adhere to the academy staff Acceptable Use Policy.
- To report any online safety related issues that come to your attention to the online safety coordinator.
- To develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.

- To support the academy in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the academy network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the academy ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on academy owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within the academy.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to academy -owned software assets is restricted.

3.5 The Designated Safeguarding Lead will be responsible for the following actions:

- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online safety contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.
- To be aware that these are child protection issues and not technical issues; technology provides additional means for child protection issues to develop.
- When an adult / pupil has reported any concerns the DSL / Deputy DSL will follow this up and log any incidents

3.6 Pupils will be responsible for the following actions:

- To know and understand academy policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand academy policies on the taking and use of mobile phones.
- To know and understand academy policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in the academy and at home.

- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in the academy and at home, including judging the risks posed by the personal technology owned and used outside the academy.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in the academy and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in the academy and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within the academy.
- To discuss online safety issues with family and friends in an open and honest way.
- Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the academy's normal behaviour or disciplinary procedures.
- Instances of cyber-bullying will be taken very seriously by the academy and dealt with using the academy anti-bullying procedures. The academy recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

3.7 Parents/Carers will be responsible for the following actions:

- To help and support the academy in promoting online safety.
- To read, understand and promote the academy pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in academy and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss online safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology
- To consult with the academy if they have any concerns about their children's use of technology.
- To agree to and sign the home-academy agreement which clearly sets out the use of photographic and video images outside of the academy.
- To sign an Online Safety Agreement

3.8 The Governing Body will be responsible for the following actions:

- To read, understand, contribute to and help promote the academy's online safety policies and guidance.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the academy ICT infrastructure provides safe access to the internet.

- To develop an overview of how the academy encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of the academy.
- To support the work of the online safety group in promoting and ensuring safe and responsible use of technology in and out of the academy, including encouraging parents to become engaged in online safety activities.
- To ensure appropriate funding and resources are available for the academy to implement its online safety strategy.
- The Governors will undertake an annual review of this policy and its procedures and of the efficiency with which the relevant duties have been discharged.

The role of the **Online Safety Governor** includes:

- Regular meetings with the Online safety lead
- Regular monitoring of online safety incident logs
- Reporting to Governors meeting
- In addition, the Designated Safeguarding Lead will monitor the operation of this policy and its procedures and report to the Online safety Governor

3.9 Other community or external users will be responsible for the following actions:

- The academy will liaise with local organisations to establish a common approach to online safety and the safe use of technologies.
- The academy will be sensitive and show empathy to internet-related issues experienced by pupils out of the academy, e.g. social networking sites, and offer appropriate advice where appropriate.
- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within the academy.
- The academy will provide an Acceptable Use Policy for any guest who needs to access the academy computer system or internet on academy grounds.
- The academy will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within the academy.

<u>Protecting the professional identity of all staff, work placement pupils and volunteers</u>

Communication between adults and between children/young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, webcams, websites, forums and blogs.

When using digital communications, staff and volunteers should:

- Only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the academy.
- Not share any personal information with a child or young person eg should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.

- Not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- Ensure that all communications are transparent and open to scrutiny.
- Be careful in their communications with children so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care (making every effort to keep personal and professional online safety lives separate).
- Not post information online safety that could bring the academy into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

4. Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- We will provide a series of specific online safety-related lessons in every year group/specific year groups as part of the ICT curriculum / PSHE curriculum / other lessons.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-academy activities.
- We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online safety tools in a safe and effective way.
- We will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign will be displayed when a pupil logs on to the academy network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.

- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- All pupils will be taught in an age-appropriate way about copyright in relation to online safety resources and will be taught to understand about ownership and the importance of respecting and acknowledging copyright of materials found on the internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online safety bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. adult / member of staff or through the confide system in academy.

All Staff (including Governors)

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

- A planned programme of formal online safety training will be made available to staff.
- An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and Acceptable Use Policies.
- The Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety lead will provide advice / guidance / training as required to individuals as required.

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 and in promoting the positive use of the internet and social media. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The academy will therefore take every opportunity to help parents understand these issues through:

- Parents' evenings
- Newsletters
- Letters
- Website
- Twitter
- Information about national/local online safety campaigns/literature

5. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupil's instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 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.
- Staff 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 pupils / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the academy website
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

6. Managing ICT Systems and Access

At Lower Meadow Primary Academy the ICT systems are managed by the technical staff contracted to the academy/ Astrea.

The academy will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible as outlined in Keeping Children Safe in Education 2023.

- All access to academy ICT systems should be based upon a 'least privilege' approach.

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The academy will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- Members of staff will access the internet using an individual id and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID and password. They will abide by the academy Acceptable Use Policy at all times.
- Incidents which create a risk to the safety of the academy network, or create an information security risk, will be referred to the academy's online safety lead and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches academy policy then appropriate sanctions will be applied. The academy will decide if parents need to be informed if there is a risk that pupil data has been lost.
- The academy reserves the right to monitor equipment or their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

7. Filtering and Monitoring Internet Access

At Lower Meadow Primary Academy the filtering system is provided by Wave 9/Sophos/DNA NetSupport. The academy ensures that the appropriate filters and monitoring systems are in place as outlined in Keeping Children Safe in Education 2023.

The Principal will ensure the appropriate Filtering and Monitoring systems are in place within the Academy IT infrastructure. The Trust has equipped all Astrea academies with Sophos filtering software which includes a firewall that monitors and filters incoming and outgoing network traffic. Sophos' main purpose is to allow non-threatening digital traffic in and to keep potentially dangerous digital traffic out. Appropriate levels of filtering can be assigned to users by using the Sophos appliance, which can be fine-tuned at each location. Astrea Trust has equipped all Astrea Academies with NetSupport DNA monitoring software. NetSupport DNA will monitor the Academy network and identify when a user triggers terminology that could indicate potential harmful or risky behaviours.

The DSL will ensure that the NetSupport DNA console is available on the devices of at least two members of the safeguarding team, and that there is a strategic plan to review and respond to triggers highlighted through NetSupport DNA.

Technology, and risks and harms related to it, evolve, and change rapidly. The DSL will carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. KCSiE 2023 recommends the 360 Safe assessment tools:

- *Risk Assessment: https://360safe.org.uk/overview/template-online-risk-assessment/*
- *Self-Assessment : https://360safe.org.uk*

At Lower Meadow Primary Academy the IT technician ensures that all device types that are available in academy and capable of serving internet content are filtered, e.g. laptops, netbooks, PCs and mobile phones.

- *The academy will always be proactive regarding the nature of content which can be viewed through the academy's internet provision.*

- *The academy will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.*

    - *Where incidents are raised on an Online Safety concern form the pupil(s) will be spoken to and parents/carers will be made aware.*

    - *If a pupil or staff try to access inappropriate material or type in inappropriate words this immediately sends an email to our IT department. Pupils, staff and parents are then made aware.*

    - *Any ICT concerns are logged and held by the Safeguarding Lead.*

    - *If users discover a website with inappropriate content, this should be reported the online safety co-ordinator. All incidents should be documented.*

    - *If users discover a website with potentially illegal content, this should be reported immediately to the online safety coordinator. The academy will report such incidents to appropriate agencies including the filtering provider, the local authority or CEOP.*

    - *The academy will regularly review the filtering product for its effectiveness.*

    - *The academy filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.*

    - *Any amendments to the academy filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.*

    - *Pupils will be taught to assess content as their internet usage skills develop.*

    - *Pupils will use age-appropriate tools to research internet content.*

    - *The evaluation of online safety content materials is a part of teaching and learning in every subject and will be viewed as a whole-academy requirement across the curriculum.*

8. Passwords

A secure and robust username and password convention exists for all system access. (email, network access, academy management information system).

- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within academy.
- All information systems require end users to change their password at first log on.
- Users should be prompted to change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise
- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- All staff and pupils will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- Admin staff will inform the IT team when staff leave as part of an exit strategy.
- Staff will be made aware of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected.
- Passwords will be discussed during initial staff inductions.

All staff and pupils will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.

- Do not write down system passwords.
- Only disclose your personal password to authorised IT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
- Always use your own personal passwords to access computer based services, never share these with other users.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Never save system-based usernames and passwords within an internet browser.
- All access to academy information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the academy's personal data policy.
- The academy maintains a log of all accesses by users and of their activities while using the system.
- Passwords must contain a minimum of eight characters and be difficult to guess.
- Users should create different passwords for different accounts and applications.
- Users should use Capital letters, numbers, letters and special characters in their passwords (! @ # $ % * ( ) - + =, < > : : " '): the more randomly they are placed, the more secure they are.

9. Management of Assets

- Details of all academy-owned hardware will be recorded in a hardware inventory.
- Details of all academy-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The academy will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

10. Data Protection

Personal Data

The academy may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about children/young people, members of staff/volunteers/pupils and mothers and fathers/carers e.g. names, addresses, contact details, legal guardianship/contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by mothers and fathers / carers or by other agencies working with families

The Data Protection Act 1998 requires every organisation processing personal data to notify with the Information Commissioner's Office, unless they are exempt. Settings that work with children and young people are likely to be under greater scrutiny in their care and use of personal data, following high profile incidents. In April 2010 the Information Commissioners Office introduced a new maximum £500K fine for breaches of information security for both public and private sector organisations. All academies must understand the implications of not securing the information assets they hold and should look to appoint a Senior Information Risk Officer (SIRO)
This role may well be combined with the academy's Data Protection Officer and, where appropriate, Information Asset Owners (IAO) Senior Information Risk Owner (SIRO) The Senior Information Risk Owner/Information Asset Owner is the Principal. They have the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)

- They act as an advocate for information risk management
- What information is held, and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why

How information is retained and disposed of 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
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.
- 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 or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The 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 academy policy once it has been transferred or its use is complete.

The academy has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within academy.

- The academy has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the academy will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO (Senior Information Risk Holder) and the applicable IAO (Information Asset Owners).

- All access to the academy information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on academy servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the academy.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the academy's information-handling procedures and, for example, not left in cars or insecure locations.

Secure Transfer Process

If you are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access.

Email

It is advisable not to use public email accounts for sending and receiving sensitive or personal data. DO NOT include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email. Encryption makes a file non readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

FAX

- Fax machines will be situated within controlled areas of the academy.
- All sensitive information or personal data sent by email or fax will be transferred using a secure method.
- Personal or sensitive information must be within the email itself as the information may be insecure. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

11. Communication technologies

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

	Staff and other adults	**Pupils / Pupils**

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed (But must be kept securely in the office through the day)	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to academy	X				x			
Use of mobile phones in lessons				X				X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones or other camera devices		X*						X
Use of hand held devices e.g. PDAs, PSP		X						X
Use of personal email addresses in academy, or on academy network		X						X
Use of academy email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of instant messaging		X						X
Use of social networking sites		X						X
Use of blogs		X						X

x*With the Principal's permission, staff may use personal devices to record school activities if their school device is unavailable. Staff must inform the principal about this,

including the reason why this was needed, make sure that photographs are sent to the school's workspace and are then deleted (as far as possible on the same day).

The official academy email service may be regarded as safe and secure and is monitored. Staff and pupils / pupils should therefore use only the academy email service to communicate with others when in academy, or on academy systems (eg by remote access).

Users need to be aware that email communications may be monitored.

Users must immediately report, to the nominated person, in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and pupils / pupils or parents / carers (email, chat, Virtual Learning Environment etc.) must be professional in tone and content.

12. Inappropriate/Unsuitable Activities

The 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 the academy or outside the academy when using academy equipment or systems. The academy policy restricts certain internet usage as follows:

User Actions		**Acceptable**	**Acceptable at certain times**	**Acceptable for certain 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					X
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X

	Adult material that potentially breaches the Obscene Publications Act in the UK					X
	Criminally racist material in UK					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Promotion of racial or religious hatred				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				X	
Using academy systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by YGFL and/or the academy					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet					X	
Online gaming (educational)					X	
Online gaming (non educational)					X	
Online shopping/commerce					X	
File sharing					X	
Use of social networking sites					X	
Use of video broadcasting eg Youtube					X	

<u>Responding to incidents of misuse</u>

It is hoped that all members of the academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation It is more likely that the 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 academy 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:

13. Legislation

Computer Misuse Act 1990

This Act makes it an offence to:

Erase or amend data or programs without authority;
Obtain unauthorised access to a computer;
"Eavesdrop" on a computer;
Make unauthorised use of computer time or facilities;
Maliciously corrupt or erase data or programs;
Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The Act states that person data must be:

Fairly and lawfully processed.
Processed for limited purposes.
Adequate, relevant and not excessive.
Accurate.
Not kept longer than necessary.
Processed in accordance with the data subject's rights.
Secure.
Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Information and support for academys as outlined in Keeping Children Safe in Education 2016 Annex C.

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

www.educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Contacts

The details of the designated officer/online safety lead is as follows:

Amy Marshall, Assistant Principal

Designated Safeguarding Lead - Maisie Edwards

All can be contacted on 0114 237 2700

Lower Meadow Primary Academy, Batemoor RS, Sheffield, S8 8EE

The telephone numbers of the Shefffield Council children's social care services departments are as follows:

West Team	0114 2374491
Safeguarding HUB (Channel included)	0114 2734855

The following telephone numbers may be useful for pupils:

Childline	0800 1111
NSPCC	0808 800 5000
Ofsted's Whistleblowing Hotline	0300 123 3155