# Online Safety Policy

| | |
|---|---|
| **Last reviewed on:** | January 2024 |
| **Next review due by:** | January 2025 |

**Aims**

Gooseacre 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 takes into account the procedures and practice of the Local Safeguarding Children Board and the Updated Keeping Children Safe in Education 2022. This policy should be used alongside the Child Protection and Safeguarding 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.

Our academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

- This policy applies to all members of the school community including staff, students, parents/carers, volunteers and work placements, who have access to and are users of school ICT (Information and Communication Technologies) systems both in and out of school.
- The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school 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 school, but is linked to membership of the school.
- The Education Act 2011 gives the school 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 school 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 school.

**2. Legislation and guidance**

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- Relationships and sex education.
- Searching, screening and confiscation.

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting

inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

**Roles and Responsibilities**

The Principal has overall responsibility for online safety of all members of the school community. Day to day responsibility will be delegated to the Online Safety Leader. The Principal will ensure that the Online Safety Leader 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 (SLT) will make themselves aware of the procedures to follow in the event of a serious online safety incident.

The Online Safety Coordinator will ensure:

- The school online safety policy is current and pertinent.
- The school online safety policy is reviewed at regular intervals.
- The school Acceptable Use policies are appropriate for their intended audience.

Responsibilities of the Online Safety Coordinator:

- To promote safe usage of the Internet and related technologies within school.
- To promote an awareness and commitment to online safety throughout the school.
- To be the first point of contact in school on all online safety matters.
- To take day-to-day responsibility for online safety within school and to have a leading role in establishing and reviewing the school online safety policies and procedures.
- To communicate regularly with the IT Support Coordinator.
- To communicate regularly with the designated 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 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.

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

- To read, understand and help promote the school's online safety policies and guidance.
- To read, understand and adhere to the school 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 school-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 which exist within the school.
- 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.

Technical Support Staff (IT Support Coordinator and External IT staff) will be responsible for the following actions:

- To read, understand, contribute to and help promote the school's online safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any online safety related issues that come to their 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 their personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for the detection of misuse and malicious attack.
- To take responsibility for the security of the school 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 school owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- 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 school owned software assets is restricted.

The Designated Safeguarding lead (DSL) 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 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.
- To have regular contact with other online safety teams, e.g. Safeguarding Children Board
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- When an adult / pupil has reported any concerns the DSL / Deputy DSL will follow this up and log any incidents

Pupils will be responsible for the following actions:

- To know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies on the taking and use of mobile phones.
- To know and understand school policies regarding cyberbullying.
- To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school 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 school and at home, including judging the risks posed by the personal technology owned and used outside school.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school 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 school.

- 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 school's normal behaviour or disciplinary procedures.
- Instances of cyber-bullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

Parents/Carers will be responsible for the following actions:

- To help and support the school in promoting online safety.
- To read, understand and promote the school 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 school 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 school if they have any concerns about their children's use of technology.
- To agree to and sign the home-school agreement which clearly sets out the use of photographic and video images outside of school.

Protecting the professional identity of all staff, work placement students and volunteers

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 school.
- Not share any personal information with a child or young person e.g. 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 that could bring the school into disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

**Education**

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

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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 (Jigsaw) / other lessons.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school 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-use Acceptable Use Policy which every pupil will sign and which will be displayed when a pupil logs on to the school 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 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 school.

All Staff (including LGC)

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 school 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 Coordinator 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 school will therefore take every opportunity to help parents understand these issues through:

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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

**Cyber-bullying**

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

**Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be, the issue will be addressed in assemblies and through the curriculum, including the PSHE scheme jigsaw.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**Anti Radicalisation and Prevent Duty**

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems at Gooseacre Primary Academy block inappropriate content, including extremist content.

**Where staff, pupils or visitors find unblocked extremist content they must report to the Designated Safeguarding Lead and E Safety Lead immediately.**

We are aware that children may have access to unfiltered content when using the internet at home, and therefore, this policy refers to preventing radicalisation and related extremist content. Pupils and staff know how to report internet content that is inappropriate or of a concern.

There is a chance a child may meet people online or visit websites that could lead to them adopting extreme views and becoming radicalised. Curiosity could lead to a child to seek out these people to they could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views / actions would be considered extreme.

There is no single driver of radicalisation, nor is there a single journey to becoming radicalised. The internet creates more opportunities to become radicalised, since it is a worldwide 24/7 medium that allows you to find and meet people who will share and reinforce opinions.

**What signs should we look out for?**

There are a number of signs to be aware of; Parents and Staff should look out for increased instances of:

- A conviction that their religion, culture or beliefs are under threat and treated unjustly.
- A tendency to look for conspiracy theories and distrust of mainstream media.
- The need for identity and belonging.
- Being secretive about who they talk to online and what sites they visit.
- Switching screens when an adult / Parent/ carer goes near their phone, tablet or computer.
- Possessing items: electronic devices, phones that parents have not given them or are aware of.
- Becoming emotionally volatile.

However it should be remembered that not all children/ young people who experience / display these factors adopt radical views.

**Referral Process:**

Staff and visitors must refer all concerns about pupils who show signs of vulnerability or radicalisation to the Designated Safeguarding Lead, as using the agreed process as stated in the Safeguarding Policy.

**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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the Internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students /pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school 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 school website.
- Pupil's work can only be published with the permission of the pupil and parents/carers.
- When searching for images, video or sound clips, pupils will be taught about copyright and acknowledging ownership.

**Remote Education**

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of online learning lessons and resources via our learning portals, e.g. Microsoft Teams.
- We expect pupils to follow the same principles, as outlined in the schools Acceptable User policy, whilst learning at home.
- When communicating with pupils online via Teams / learning portals this will be done so with the approval of the Principal and only at the pre-agreed times. There will be two staff members to each live learning session and these will be recorded.
- Pupils must uphold the same level of behavioural expectations as they would in a normal classroom setting.
- Any significant behavioural issues occurring on any virtual platform must be reported and appropriate sanctions will be applied.

**Managing ICT Systems and Access**

At Gooseacre Primary Academy the ICT systems are managed by the IT Support Coordinator in association with the School Business Manager.

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible as outlined in the updated Keeping Children Safe in Education 2021.

- All access to school 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 school 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 school Acceptable Use Policy at all times.

- Incidents which create a risk to the safety of the school network, or create an information security risk, will be referred to the school's Online Safety Coordinator and IT Support Coordinator. Appropriate advice will be sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data security has been compromised.
- The school reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

**Filtering Internet Access**

At Gooseacre Primary Academy the filtering system is provided by Wave9 Managed Services Ltd. The school ensures that the appropriate filters and monitoring systems are in place as outlined in updated Keeping Children Safe in Education 2022. The IT Support Coordinator will ensure that all device types that are available in school and capable of serving internet content (via the school's internet connection) are filtered, e.g. laptops, netbooks, PCs and mobile phones.

- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school 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 will be recorded automatically by the filtering system and an email notification sent to the IT Support Coordinator and Online Safety Coordinator. The DSL will be notified if appropriate and action taken in accordance with normal procedures. Pupils, staff and parents may then also be made aware.
- Any online safety concerns are logged and held by the Safeguarding Lead.
- If users discover a website with inappropriate content, this should be reported the Online Safety Coordinator. 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 school will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the IWF.
- The school will regularly review the filtering product for its effectiveness.
- The school filtering system will block all sites on the Internet Watch Foundation list and this will be updated daily.
- Any amendments to the school 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 content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

**Passwords**

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

- All Pupils will have a generic 'pupil' logon to all school ICT equipment when required.
- For access to some equipment and services, pupils may also be issued with a unique user account and password.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- All school-based information systems require end users to change their password at first log on. Most externally hosted systems have similar security features.
- 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.
- Office staff will inform the IT Support Coordinator and Astrea Central IT support 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.
- All access to school 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 school's personal data policy.
- The school 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.

**Management of Assets**

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-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 school 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.

**Data Protection**

Personal Data

The school 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/students 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.

The Senior Information Risk Owner/Information Asset Owner 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.
- They know what information is held, and for what purposes.
- They are aware how information will be amended or added to over time.
- They understand who has access to the data and why.

All personal data must be recorded, processed, transferred, disposed of 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.

Authorised users of personal data must:

- 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 and that their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices or services
- 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 offer approved virus and malware checking software.
- The data must be securely deleted from the device, in line with school policy, once it has been transferred or its use is complete.

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

- The school has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the school 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 school 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 school 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 school.
- 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 school's information handling procedures and, for example, not left in cars or insecure locations.

**Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

**Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

**How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Safeguarding and behaviour. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**Training**

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL [and deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

**Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by Astrea Academy Trust, the Principal and the DSL. At every review, the policy will be shared with the LGC.