# GILLINGSTOOL PRIMARY SCHOOL

*Inspire ~ Believe ~ Achieve*

# COMPUTING AND ONLINE SAFETY POLICY

Name: Nicola Thomerson and Alison Williams

Co-Chair of Academy Community Council

Date: March 2025

Name: Caroline Carter

Headteacher

Date: March 2025

## Academy Community Councillors

Academy Community Councillors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Academy Community Councillors receiving regular information about e-safety incidents and monitoring reports. A member of the Academy Community Council has taken on the role of Safeguarding Councillor. The role of the Safeguarding Councillor will include:

- Regular meetings with the computing subject lead;
- Regular monitoring of e-safety incident logs;
- Reporting to relevant Academy Community Councillors.

## Headteachers and Senior Leaders

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community. The Headteacher/Senior Leaders are responsible for ensuring that the E-Safety Coordinator/Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Senior Leadership Team will receive regular monitoring reports from the Computing Subject Lead.

## E-Safety/Computing Subject Lead

The E-Safety/Computing Subject Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Provides training and advice for staff;
- Liaises with the IT provider;
- Liaises with school ICT technical staff;
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Meets regularly with Safeguarding Councillor to discuss current issues, review incident logs and filtering/change control logs;
- Attends relevant meeting/committee of Academy Community Councillors;
- Reports regularly to Senior Leadership Team.

## Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- They have read, understood the school Staff Acceptable Use Policy/Agreement (AUP);
- They report any suspected misuse or problem to the E-Safety lead
- Digital communications with students/pupils (email) should be on a professional level and only carried out using official school systems;
- E-safety issues are embedded in all aspects of the curriculum and other school activities;
- Pupils understand and follow the school e-safety and acceptable use policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extracurricular and extended school activities;
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

## Designated Safeguarding Lead

The Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate on-line contact with adults/strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying.

## Students and pupils

Students and pupils are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.

Pupils will:

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of IT 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 e-safety campaigns/literature.

## Policy Statements

### 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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Planned e-safety lessons should be provided as part of computing lessons at the beginning of each term.
- Key e-safety messages should be reinforced as part of assemblies;
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
- Pupils should be helped to understand the need for the/ pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

### Education – parents and carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, website;
- Parents evenings;
- Reference to the SWGfL "Golden Rules" for parents).

## Education and Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly;
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety and Computing Policy and Acceptable Use Policies;
- The Computing Subject Lead will receive regular updates through attendance at information/training sessions and by reviewing guidance documents released by Mosaic Partnership Trust and others;
- This E-Safety and Computing Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days;
- The Computing Subject Lead will provide advice/guidance/training as required to individuals as required.

## Training – Academy Community Councillors

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

- Attendance at training provided by the Mosaic Partnership Trust/National Governors Association/SWGfL or other relevant organisation;
- Participation in school training/information sessions for staff or parents.

## Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities.

- School IT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the school Security Policy and Acceptable Usage Policy and any relevant trust policy and guidance;
- There will be regular reviews and audits of the safety and security of school IT systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to school IT systems;
- All users will be provided with a username and a password where necessary by the Network Manager who will keep an up to date record of users and their usernames;
- Users will be made responsible for the security of their username and password, 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;
- The school maintains and supports the managed filtering service provided by Integra IT;
- Any filtering issues should be reported immediately to Integra IT;
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy;

- Remote management tools are used by Network Managers /staff to control workstations and view user's activity;
- An appropriate system (CPOMs) is in place for users to report any actual/potential e-safety incident to the DSL/DDSL;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data;
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system;
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on laptops and other portable devices that may be used out of school;
- An agreement is in place that allows staff installing programmes on school workstations/portable devices;
- The school infrastructure and individual workstations are protected by up to date virus software;
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of IT across the curriculum;

- In lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit;
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need;
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information;
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff 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 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;
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or 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;

## Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (2018) 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.

**Staff must ensure that they:**

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**

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 (many memory sticks/cards and other mobile devices cannot be password protected);
- The device must offer approved virus and malware checking software;
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

## Communications

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

| | Staff & other adults | | | | Students/Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school | √ | | | | √ | | | |
| Use of mobile phones in lessons | | | | √ | | | | √ |
| Use of mobile phones in social time | √ | | | | | | | √ |
| Taking photos on mobile phones or other camera devices | √ | | | | | | | √ |
| Use of hand held devices eg PDAs, PSPs | | √ | | | | √ | | |
| Use of personal email addresses in school, or on school network | √ | | | | | | | √ |
| Use of school email for personal emails | √ | | | | | | √ | |
| Use of chat rooms/facilities | | | | √ | | | | √ |
| Use of instant messaging | | | | √ | | | | √ |
| Use of social networking sites | | | | √ | | | | √ |
| Use of blogs | | √ | | | | | √ | |

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

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school 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 students/pupils or parents/carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Whole class or group email addresses will be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be

reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

## User Actions

| | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| **Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:** | **child sexual abuse images** | | | | | ☐ |
| | **promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation** | | | | | ☐ |
| | **adult material that potentially breaches the Obscene Publications Act in the UK** | | | | | ☐ |
| | **criminally racist material in UK** | | | | | ☐ |
| | **pornography** | | | | ☐ | |
| | **promotion of any kind of discrimination** | | | | ☐ | |
| | **promotion of racial or religious hatred** | | | | ☐ | |
| | **threatening behaviour, including promotion of physical violence or mental harm** | | | | ☐ | |
| | **any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute** | | | | ☐ | |
| **Using school systems to run a private business** | | | | | ☐ | |
| **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Integra IT and/or the school** | | | | | ☐ | |
| **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions** | | | | | ☐ | |
| **Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords)** | | | | | ☐ | |
| **Creating or propagating computer viruses or other harmful files** | | | | | ☐ | |
| **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** | | | | | ☐ | |
| **On-line gaming (educational)** | | | √ | | | |
| **On-line gaming (non educational)** | | | | | √ | |
| **On-line gambling** | | | | | √ | |
| **On-line shopping/commerce** | | | √ | | | |
| **File sharing** | | | √ | | | |
| **Use of social networking sites** | | | | | √ | |
| **Use of video broadcasting eg Youtube** | | | √ | | | |

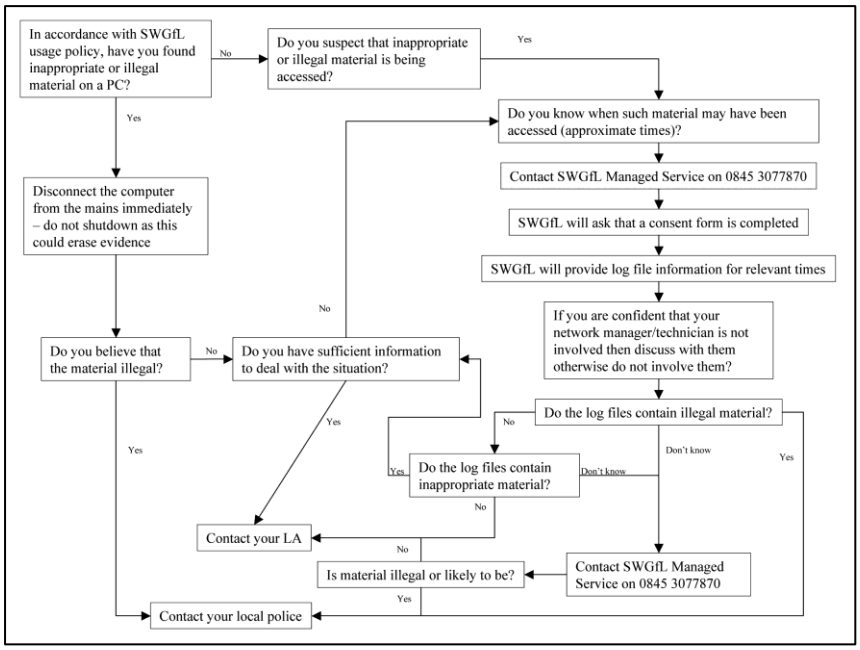
## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of IT, 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 ie.**

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

**the SWGfL flow chart – below and http://www.swgfl.org.uk/safety/default.asp should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.**




If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

## Pupils Actions/Sanctions

| Incidents: | Refer to class teacher/tutor | Refer to Head of Department/Head of Year/other | Refer to Headteacher | Refer to Police | Refer to technical support staff for action re filtering/security etc | Inform parents/carers | Removal of network/internet access rights | Warning | Further sanction eg detention/exclusion |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).** | √ | | √ | √ | | √ | | | √ |
| Unauthorised use of non-educational sites during lessons | √ | | √ | | √ | √ | | | |
| Unauthorised use of mobile phone/digital camera/other handheld device | √ | | √ | | | √ | | | √ |
| Unauthorised use of social networking/instant messaging/personal email | √ | | √ | | | √ | | | √ |
| Unauthorised downloading or uploading of files | v | | √ | | | | | | |
| Allowing others to access school network by sharing username and passwords | √ | | √ | | | | | | |
| Attempting to access or accessing the school network, using another student's /pupil's account | √ | | √ | | | | | | |
| Attempting to access or accessing the school network, using the account of a member of staff | √ | | √ | | √ | √ | | | √ |
| Corrupting or destroying the data of other users | √ | | √ | | √ | √ | | | √ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | √ | | √ | √ | √ | √ | | | √ |
| Continued infringements of the above, following previous warnings or sanctions | √ | | √ | √ | √ | √ | | | √ |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | √ | | √ | | √ | √ | | | √ |
| Using proxy sites or other means to subvert the school's filtering system | √ | | √ | | √ | √ | | | √ |
| Accidentally accessing offensive or pornographic material and failing to report the incident | √ | | √ | | √ | √ | | | |
| Deliberately accessing or trying to access offensive or pornographic material | √ | | √ | √ | √ | √ | | | √ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the General Data Protection Regulation | √ | | √ | | √ | √ | | | √ |

## Staff Actions/Sanctions

| Incidents: | Refer to line manager | Refer to Headteacher | Refer to Local Authority/HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).** | | √ | √ | √ | √ | | | √ |
| Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email | | √ | | | √ | √ | | |
| Unauthorised downloading or uploading of files | | √ | √ | | √ | √ | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | | √ | | | | | | |
| Careless use of personal data eg holding or transferring data in an insecure manner | | √ | | | | | | |
| Deliberate actions to breach data protection or network security rules | | √ | √ | | √ | | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | √ | √ | √ | | | | √ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | √ | √ | √ | | | | √ |
| Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils | | √ | | | √ | √ | | |
| Actions which could compromise the staff member's professional standing | | √ | √ | | | √ | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | √ | √ | | | √ | | |
| Using proxy sites or other means to subvert the school's filtering system | | √ | √ | | √ | √ | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | √ | √ | | √ | √ | | |
| Deliberately accessing or trying to access offensive or pornographic material | | √ | √ | √ | √ | | | √ |
| Breaching copyright or licensing regulations | | √ | | | | √ | | |
| Continued infringements of the above, following previous warnings or sanctions | | √ | √ | | | | | √ |

## School Filtering Policy

Integra IT schools automatically receive a filtered broadband service.

## Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so.

As a part of the Integra IT schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

## Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Computing coordinator. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

All users have a responsibility to report immediately to the Computing coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

## Education/Training/Awareness

Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- *the AUP*
- *staff meetings, briefings, Inset.*

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions/newsletter etc.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT coordinator who will decide whether to notify Integra IT. If it is felt that the site should be filtered (or unfiltered) at county level, the responsible person should email Integra IT with the URL.

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use agreement.

## Audit/Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- *E-Safety Councilor/Academy Community Council*
- *Integra IT/Mosaic Partnership Trust on request*

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

## Policy Statements

The school will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.

Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

## Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be 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 members of the school community – including *pupils/students*, members of staff and parents and carers e.g. names, addresses, contact details, legal guardianship/contact details, health records, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Academy Community Councillors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as an Academy Community Councillor.

## Training and Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings/briefings/Inset

## Secure Storage of and Access to Data

The school will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.

All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (ie owned by the users) must not be used.
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 (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

All paper based IL2-Protected and IL3-Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the General Data Protection Regulation (2018), data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests ie. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

## Secure Transfer of Data and Access Out of School

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA/school policies may forbid such transfer);
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school;

- When data is required by an authorised user from outside the school premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software;
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority in this event.

## Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance (see further reading section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.

*A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

## Audit Logging/Reporting/Incident Handling

As required by the "Data Handling Procedures in Government" document, the activities of data users, in respect of electronically held personal information, will be logged and these logs will be monitored by responsible individuals. (Chair of Academy Community Council and Headteacher)

The audit logs will be kept to provide evidence of accidental or deliberate security breaches – including loss of protected data or breaches of an acceptable use policy, for example. Specific security events should be archived and retained at evidential quality for seven years.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

## Our School Community

Discusses, monitors and reviews our e-safety **policy** on a regular basis. Good practice suggests the policy should be reviewed every three years.

Supports **staff** in the use of IT as an essential tool for enhancing learning and in the embedding of e-safety across the whole school curriculum.

Ensures that **pupils** are aware, through e-safety education, of the potential e-safety risks associated with the use of IT and mobile technologies, that all e-safety concerns will be dealt with sensitively and effectively; that pupils feel able and safe to report incidents; and that pupils abide by the school's e-safety policy.

Provides opportunities for **parents/carers** to receive e-safety education and information, to enable them to support their children in developing good e-safety behaviour. The school will report back to

parents/carers regarding e-safety concerns. Parents/carers in turn work with the school to uphold the e-safety policy.