# Ursula Taylor C of E  School

Living God's Love, Together We Flourish

## E- Safety and Data Security

## Acceptable Use Policy

**Updated February 2021**

## Review due February 2023

## Contents

| | Page Number: |
|---|---|
| Introduction | 4 |
| Monitoring | 5 |
| Breaches | 6 |
| Incident Reporting / Whistle Blowing | 6 |
| UTPS Pupil Acceptable Use Agreement / eSafety Rules | 7 |
| Parent Letter re: AUP | 8 |
| Staff, Governor , Visitor AUP Agreement | 9 |
| Professional Responsibilities | 10 |
| Computer Viruses | 11 |
| Data Security | 11 |
| Protective Marking of Official Information | 11 |
| Disposal of Redundant ICT Equipment Policy | 12 |
| Email | 13 |
| Managing Email | 13 |
| Receiving Emails | 14 |
| Emailing personal or confidential Information | 15 |
| Equal Opportunities | 15 |
| eSafety and Roles and Responsibilities | 16 |
| eSafety in the Curriculum | 16 |
| eSafety Skills development for staff | 17 |
| Managing the school eSafety messages | 17 |
| eSafety Incident Log | 17 |
| Misuse and Infringements | 17 |
| Complaints | 17 |
| Inappropriate Material | 17 |
| Internet Access | 18 |
| Managing the Internet | 18 |
| Internet Use | 18 |
| Infrastructure | 18 |
| Managing other online technologies | 19 |
| Parental Involvement | 20 |
| Passwords and Password security | 21 |
| Passwords | 21 |
| Password Security | 21 |
| Zombie Accounts | 22 |

| | |
|---|---|
| Personal or Sensitive Information | 22 |
| Storing / Transferring Personal or Sensitive Information using Removable Media | 22 |
| Remote Access | 23 |
| Safe use of Images | 23 |
| Taking of Images and Film | 23 |
| Consent of adults Who Work at the School | 23 |
| Publishing Pupil's Images and Work | 24 |
| Storage of Images | 24 |
| Webcams and Surveillance Cameras | 24 |
| Video Conferencing | 25 |
| School ICT Equipment including Portable and Mobile ICT Equipment and Removable Media | 25 |
| Portable and Mobile ICT equipment | 26 |
| Mobile Technologies | 26 |
| Personal Mobile Devices (including Phones) | 27 |
| School provided Mobile Devices (including phones) | 27 |
| Telephone Services | 27 |
| Removable Media | 28 |
| Servers | 28 |
| Social Media, including Facebook and Twitter | 28 |
| Systems and Access | 29 |
| Writing and Reviewing this Policy | 30 |
| Appendix – Summary of Policy | 31 |

## INTRODUCTION

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults.  Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning.  It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole.  Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat/gaming apps

- Social Media, including Facebook/Twitter/Instagram
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Ursula Taylor C of E School, we understand the responsibility to educate our pupils on eSafety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

## **MONITORING**

Authorised Staff at Ursula Taylor C of E School are:

Mrs V Morrall – Headteacher

Ms K Hall – Deputy Headteacher

Mrs H Lee – Assistant Headteacher

Miss D Daley – Office Manager

Mrs T Mulholland – School Business Manager

Any employee of Insight IT Support given permission by any of the staff members named above.

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the General Data Protection Regulations, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

## BREACHES

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner’s powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay fines for serious breaches of the GDPR.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations’ processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For breaches committed by a child at Ursula Taylor C of E School, the school Behaviour Policy and procedures will apply.

**Incident Reporting / Whistle-Blowing**

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school’s relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Mrs V Morrall – Headteacher, Ms K Hall – Deputy Headteacher, Mrs H Lee – Assistant Headteacher and Miss Debbie Daley – Office Manager.

Please refer to the relevant section on Incident Reporting/ Whistle- Blowing, eSafety Incident Log & Infringements.

## Ursula Taylor C of E School - Pupil Acceptable Use Agreement / eSafety Rules

- I will only use ICT in school for school purposes

- I will only use my class email address or my own school email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not sign up to online services until I am old enough

High Street, Clapham, Bedfordshire, MK41 6EG Tel: 01234 359128/326251
e-mail: office@ursulataylor.bedssch.co.uk

Dear Parent/ Carer

ICT including the internet, email and mobile technologies has become an important part of learning in our school.   We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.  If you have any concerns or would like some explanation please contact your child's class teacher or Mrs Morrall, Mrs Hall or Mrs Lee.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

**Thank you for your ongoing support and vigilance when using ICT at home.**

**Kind Regards**

**Mrs V Morrall**

---

**Parent/ carer signature**

We have discussed this document with …………………………………….........(child's name) and we agree to follow the eSafety rules and to support the safe use of ICT at Ursula Taylor C of E School.

Parent/ Carer Signature …….………………….………………………….

Class …………………………………  Date ………………………………

## Staff, Governor and Visitor

**Acceptable Use Agreement / Code of Conduct**

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs V Morrall.

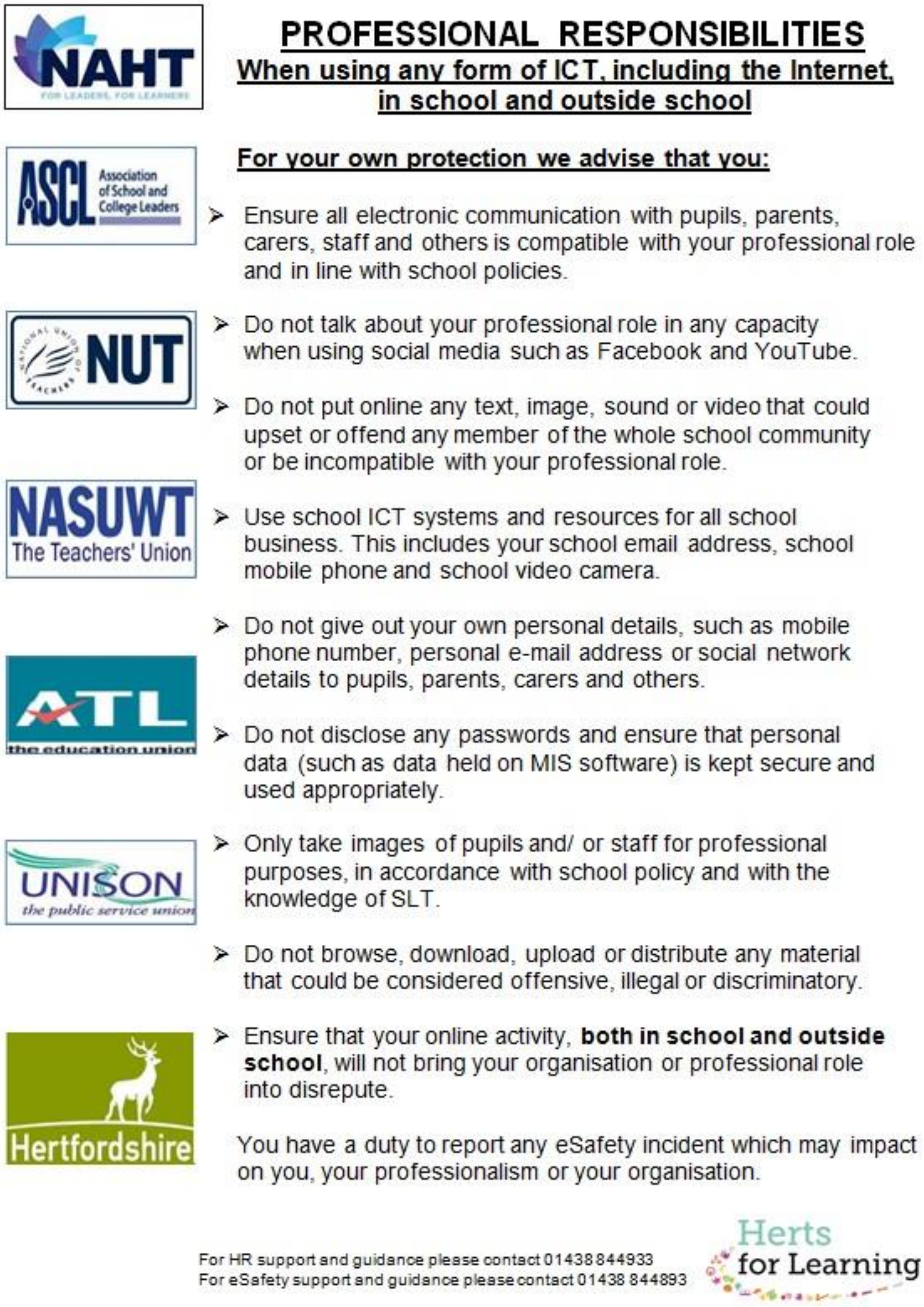
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal email address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure email system(s) for any school business
- I will ensure that personal data (such as data held on SIMs software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of Mrs V Morrall
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to a Senior leader or Headteacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I will not use personal electronic devices in public areas of the school between the hours of 8.30am and 3.30pm, except in the staff room or school office.
- I understand this forms part of the responsibilities set out in the Ursula Taylor C of E School Staff Handbook. Any disregard for the above rules by a staff member will be dealt with in accordance with the schools Disciplinary Procedure.

**User Signature**

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ………………………………………………………………….. Date ……………………………………………………….

Full Name …………………………………………………………….. (printed) Job title ………………………………………



## PROFESSIONAL RESPONSIBILITIES

### When using any form of ICT, including the Internet, in school and outside school

**For your own protection we advise that you:**

- Ensure all electronic communication with pupils, parents, carers, staff and others is compatible with your professional role and in line with school policies.
- Do not talk about your professional role in any capacity when using social media such as Facebook and YouTube.
- Do not put online any text, image, sound or video that could upset or offend any member of the whole school community or be incompatible with your professional role.
- Use school ICT systems and resources for all school business. This includes your school email address, school mobile phone and school video camera.
- Do not give out your own personal details, such as mobile phone number, personal e-mail address or social network details to pupils, parents, carers and others.
- Do not disclose any passwords and ensure that personal data (such as data held on MIS software) is kept secure and used appropriately.
- Only take images of pupils and/ or staff for professional purposes, in accordance with school policy and with the knowledge of SLT.
- Do not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Ensure that your online activity, **both in school and outside school**, will not bring your organisation or professional role into disrepute.

You have a duty to report any eSafety incident which may impact on you, your professionalism or your organisation.

For HR support and guidance please contact 01438 844933
For eSafety support and guidance please contact 01438 844893

## COMPUTER VIRUSES

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

## DATA SECURITY

- **Security**
- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal or sensitive information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used
- Anyone sending a confidential or sensitive fax should notify the recipient before it is sent

**Protective Marking of Official Information**

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation’s discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL–SENSITIVE'**

**Relevant Responsible Persons**

Senior members of staff should be familiar with information risks and the school's response.

The relevant responsible persons for Ursula Taylor C of E School are:

Mrs V Morrall – Headteacher

Ms K Hall – Deputy Headteacher

Miss D Daley – Office Manager

Mrs T Mulholland – School Bursar

- they lead on the information risk policy and risk assessment / risk register
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

## DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- All redundant ICT equipment will be disposed of through an authorised agency. This should 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 over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We 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
The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

GDPR 2018
https://ico.org.uk/for-organisations/education/
Electricity at Work Regulations 1989
http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:

    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media? *
    - How it was disposed of e.g. waste, gift, sale
    - Name of person & / or organisation who received the disposed item

* if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

**<u>EMAIL</u>**

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and how to behave responsible online.

Staff should use a school email account for all official communication to ensure that children are protected through the traceability of all emails through the school email system. In addition, it is important that staff are protected against possible allegations of inappropriate contact with children. This is to help mitigate the chance of issues occurring and is an essential element of the safeguarding agenda.

The Governors at Ursula Taylor C of E School are not provided with any confidential information regarding children through email. Documents that are required for Governor ratification are only sent by email if their contents are not confidential. Some documents relating to school information – but not detailing individual children are uploaded to the secure Governor Hub. Documents are, as far as is practicable, anonymised prior to presentation to Governors.

**Managing email**

- The school gives all staff their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business

using personal email addresses

- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper

- Staff sending emails to external organisations, parents or pupils are advised to cc. a member of the Senior Leadership Team.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 / Subject Access Request (SAR) under GDPR. You must therefore actively manage your email account as follows:

  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives

- No children at Ursula Taylor C of E School have their own email accounts. However, we have plans for the future to equip our children with emails accounts. When this has been completed, this section of the policy will be reviewed and updated. When the accounts are active the following will be expected:

- The forwarding of chain emails is not permitted in school. However the school has set up a dummy account (*specific address to be added*) to allow pupils to forward any chain emails causing them anxiety. No action will be taken with this account by any member of the school community

- All pupil email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email

- Staff must inform (the eSafety coordinator - Mrs V Morrall / Ms K Hall or Mrs H Lee) if they receive an offensive email

- Pupils are introduced to email as part of the Computing Programme of Study

- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

**Receiving emails**

- Check your email regularly

- Activate your 'out-of-office' notification when away for extended periods

- Never open attachments from an untrusted source; consult your network manager first

- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

- The automatic forwarding and deletion of emails is not allowed

**Emailing Personal or Confidential Information**

- Where your conclusion is that email must be used to transmit such data:

**Either**:
Speak to Miss D Daley who will be able to advise you of the best route to use, or send the data, if appropriate through our secure access routes.

**Or:**
Obtain express consent from your manager to provide the information by email and exercise caution when sending the email and always follow these checks before releasing the email:

- Encrypt and password protect. See http://www.thegrid.org.uk/info/dataprotection/#securedata
- Verify the details, including accurate email address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to email requests for information
- Do not copy or forward the email to any more recipients than is absolutely necessary

- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an email
- Provide the encryption key or password by a **separate** contact with the recipient(s)
- Do not identify such information in the subject line of any email
- Request confirmation of safe receipt

## EQUAL OPPORTUNITIES

**Pupils with Additional Needs**

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

## ESAFETY

### eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Mrs V Morrall / Ms K Hall / Mrs H Lee who have been designated this role as members of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinators to keep abreast of current issues and guidance through organisations such as BCC, Herts for Learning Ltd, CEOP (Child Exploitation and Online Protection) and Childnet.

Staff and governors are updated by the eSafety co-ordinators and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour (including the anti-bullying) policy and PSHCE.

### eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in Computing/ICT/ PSCHE lessons. Each Class Teacher has responsibility for the planning, maintaining and annotation of plans, assessments and documents for their class / year group.
- The school provides opportunities within a range of curriculum areas to teach about eSafety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or the 'CEOP report abuse' button

**eSafety Skills Development for Staff**

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of updates at Staff Meetings and where appropriate, whole school Training Days.

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community (see eSafety Coordinator)

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

**Managing the School eSafety Messages**

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used

- The eSafety policy will be introduced to the pupils at the start of each school year

- eSafety posters will be prominently displayed

- The key eSafety advice will be promoted widely through school displays, newsletters, class activities and so on

- We will participate in Safer Internet Day every February, and have done for a number of years.

**eSafety Incident Log**

Keeping an incident log can be a good way of monitoring what is happening and identify trends or specific concerns. The UTS eSafety Incidents Log is kept in the HTs office with the behaviour/homophobic / racist incident log.

**Misuse and Infringements**

**Complaints**
Complaints and/ or issues relating to eSafety should be made to the eSafety co-ordinators. Incidents should be logged and the **Hertfordshire Flowcharts for Managing an eSafety Incident** should be followed. (Appendices)

**Inappropriate Material**

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to one of the eSafety co-ordinators
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences – this procedure will be in line with the schools disciplinary procedures.

## INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internet use through the Bedford Borough Council Internet Service is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

### Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

- Staff will preview any recommended sites, online services, software and apps before use

- Searching for images through open search engines is discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

### Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application

- On-line gambling or gaming is not allowed

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated

**Infrastructure**

- Our school also employs some additional web-filtering which is the responsibility of Bedford Borough Council Broadband Services.
- Ursula Taylor C of E School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; GDPR, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinators or teacher as appropriate
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from Mrs V Morrall or Mrs H Lee.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed.

## MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking and online games websites to pupils within school. Access to Social networking is strictly prohibited by staff and children.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email

address, specific hobbies/ interests)

- Our pupils are advised that they are not old enough to have online profiles, however, we advise parents to ensure they set and maintain their online profiles to maximum privacy and deny access to
- Our pupils are asked to report any incidents of Cyberbullying to the school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Headteacher
- When signing up to online services that require the uploading of what could be deemed as personal or sensitive data, schools should check terms and conditions regarding the location of storage. Please see the Safe Harbor Agreement Statement http://www.thegrid.org.uk/info/dataprotection/#data
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

**PARENTAL INVOLVEMENT**

We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss eSafety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)
- Parents/carers are expected to sign a Home School agreement containing information similar to the following:
    - → I/we will support the school approach to online safety and not upload or add any text, image, sound or videos that could upset or offend any member of the school community, or bring the school name into disrepute.
    - → I/we will ensure that my/our online activity would not cause the school, staff, pupils or others distress or bring the school community into disrepute.
    - → I/we will support the school's policy and help prevent my/our child/children from signing up to services such as Facebook, Instagram, Snapchat and YouTube (edit/add services of particular concern here) whilst they are underage (13+ years in most cases).
    - → I/we will close online accounts if I/we/teachers find that these accounts are active for our underage child/children.
- The school disseminates information to parents relating to eSafety where appropriate in the form of;

- Information evenings
- Practical training sessions e.g. current eSafety issues
- Posters
- School website information
- Newsletter items

## PASSWORDS AND PASSWORD SECURITY

### Passwords

- **Always use your own** personal passwords

- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

- Staff should change temporary passwords at first logon

- Change passwords whenever there is any indication of possible system or password compromise

- Do not record passwords or encryption keys on paper or in an unprotected file

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

- Never tell a child or colleague your password

- If you aware of a breach of security with your password or account inform Mrs V Morrall, Ms K Hall or Mrs H Lee immediately

### Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security

- Users are provided with an individual network, email and Management Information System (where applicable) log-in username.

- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS (SIMs) systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)
- In our school, all ICT password policies are the responsibility of **the Class Teachers** and all staff and pupils are expected to comply with the policies at all times

**Zombie Accounts**

Zombie accounts refers to accounts belonging to all users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left
- Prompt action on disabling accounts will prevent unauthorised access
- Regularly change generic passwords to avoid unauthorised access
- Only the HT and School Bursar have external access to school systems through FPS (Financial Planning Systems) and a VPN for the HT. This is to ensure the school can function during a time of crisis and in line with our Risk Register and Business Continuity Plan.

## PERSONAL OR SENSITIVE INFORMATION

**Protecting Personal or Sensitive Information**

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal or sensitive information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal or sensitive information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal or sensitive information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling

**Storing/Transferring Personal or Sensitive Information Using Removable Media**

- Ensure removable media is purchased with encryption.
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Use BBC Secure systems for data transfers or encrypt all files containing personal or sensitive data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

## REMOTE ACCESS

- You are responsible for all activity via your remote access facility
- Only the Headteacher and School Business Manager have remote access to the servers, Financial records and Personal Information. This is solely to ensure the functionality of the school in a time of crisis and the school is unable to be accessed.
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is
- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

## SAFE USE OF IMAGES

**Taking of Images and Film**

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school’s network and deleted from the staff device
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to

record images of pupils, staff and others without advance permission from the Headteacher

- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication

**Consent of Adults Who Work at the School**

- Permission to use images of all staff who work at the school is sought on a case by case basis as and when relevant

**Publishing Pupil's Images and Work**

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site within publications and only with direct permission from parents
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Headteacher has authority to upload to the internet.

**Storage of Images**

- Images/ films of children are stored on the school's network and Interactive Learning Diary
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- Class Teachers have the responsibility of deleting the images when they are no longer required, or when the pupil has left the school

**Webcams and Surveillance Cameras**

- The school uses external surveillance cameras for security and safety. The only people with access to this are Mr R Knights – Site Manager, Mrs T Mulholland – School Business Manager, Miss D Daley – Office Manager and Mrs V Morrall – Headteacher. Notification of camera use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams will not be used for broadcast on the internet without prior parental consent
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)
- The term 'webcam' includes any device with the capacity to record video – e.g. laptops, cameras, ipod touches and ipads.

**Video Conferencing**

If video conferencing is deemed necessary by a staff member to expand the educational experiences of the children. It may only be used following the express permission of the Headteacher. This following statements must be completed and documented.

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All pupils are supervised by a member of staff when video conferencing
- The school keeps a record of video conferences, including date, time and participants
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

## <u>SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT & REMOVABLE MEDIA</u>

**School ICT Equipment**

- As a user of the school ICT equipment, you are responsible for your activity

- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory
- Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- Privately owned ICT equipment should not be used on a school network
- On termination of employment, resignation or transfer, return all ICT equipment to your Manager. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:
  - maintaining control of the allocation and transfer within their unit
  - recovering and returning equipment when no longer needed
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and General Data Protection Act

**Portable & Mobile ICT Equipment**

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades

- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

**Mobile Technologies**

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

**Personal Mobile Devices (including phones)**

- The school allows staff to bring in personal mobile phones for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Pupils are not allowed to bring personal mobile devices/phones to school.

- The school is not responsible for the loss, damage or theft of any personal mobile device

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

## School Provided Mobile Devices (including phones)

At Ursula Taylor C of E School we have one school mobile phone which has no camera or internet capability. It is used when staff are on a school trip to text or telephone if required. The only time staff should use their personal mobile phones is in a situation when the school phone is not working or has no signal.

- The sending of inappropriate text messages between any member of the school community is not allowed

- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school

- Never use a hand-held mobile phone whilst driving a vehicle

**TELEPHONE SERVICES**

- You may make or receive personal telephone calls in designated places – Staffroom or School Office.

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases

- Ensure that you are available to take any pre-planned incoming telephone calls

**Removable Media**

If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal or Sensitive Information Using Removable Media'

- Always consider if an alternative solution already exists
- Only use recommended removable media
- Encrypt and password protect
- Store all removable media securely
- Removable media must be disposed of securely by your ICT support team

**SERVERS**

- Always keep servers in a locked and secure environment

- Limit access rights

- Always password protect and lock the server

- Existing servers should have security software installed appropriate to the machine's specification

- Backup tapes should be encrypted by appropriate software

- Data must be backed up regularly

- Backup tapes/discs must be securely stored in a fireproof container

- Back up media stored off-site must be secure
- Remote backups should be automatically securely encrypted.

**SOCIAL MEDIA, INCLUDING FACEBOOK AND TWITTER**

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- At Ursula Taylor C of E School we do not use Facebook to communicate with parents and carers. Although we do have a school Twitter account which we use to share school events with parents/carers.
- Staff are not permitted to access their personal social media accounts using school equipment at any time during school hours.
- Pupils are not permitted to access social media accounts whilst at school – our children are too young to have access to most sites.
- Staff, governors, pupils, parents and carers are provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

**SYSTEMS AND ACCESS**

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time

- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or BCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

## WRITING AND REVIEWING THIS POLICY

### Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use through class discussions, ICT lessons, Staff Meetings, newsletters to parents/carers and Governing Body meetings.

### Review Procedure

There will be on-going opportunities for staff to discuss with the eSafety coordinator any eSafety issue that concerns them

There will be on-going opportunities for staff to discuss with a member of SLT any issue of data security that concerns them

This policy will be reviewed every 24 months and consideration will be given to the implications for future whole school development planning

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

This policy has been read, amended and approved by the staff, head teacher and governors in

February 2021

Review Date February 2023

Appendix

# Ursula Taylor eSafety, Data Security and Acceptable Use Policy Summary

- At UTS we have an Acceptable Use policy which is reviewed at least biannually, which all staff sign. Copies are kept on file. We use the Hertfordshire County Council model policy.
- ICT Acceptable Use Agreements are signed by all Staff/Governors/Children and Visitors (where applicable). We use the Hertfordshire County Council model agreements.
- Safe Handling of Data Guidance documents are issued to all members of the school who have access to sensitive or personal data.

Personal or sensitive material must be encrypted if the material is to be removed from the school

- At UTS we avoid data removal of sensitive material. Where it is removed it must be done on an encrypted flash drives.
- At UTS we use AVCO to securely transfer CTF pupil data files to other schools.
- At UTS we follow LA guidelines for the transfer of any other internal data transfer, using S2S, AVCO or CTF transfer

Personal or sensitive material must be held in a lockable storage area or cabinet if in an un-encrypted format (such as paper)

- At UTS we store such material in lockable filing cabinets in a secure area.
- At UTS all servers are in a lockable location and managed by DBS checked staff.
- At UTS we use follow LA back-up procedures and backups are encrypted and stored in a secure location
- At UTS we use DWM technical Solutions for disaster recovery on our admin server.

Disposal: personal or sensitive material electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

- At UTS we use the Authority's recommended current disposal firm for disposal of system hard drives where any protected or restricted data has been held.
- At this school paper based sensitive information is shredded, using cross cut shredders.
- Laptops used by staff at home (loaned by the school) where used for any protected data are brought in and disposed of through the same procedure.

- SuperUsers with access to setting-up usernames and passwords which enable users to access data systems e.g. for email, network access, and access are controlled by the Headteacher or Insight IT Support.

- Security policies are reviewed and staff updated at least annually and staff know to whom they should report any incidents where data protection may have been compromised